Available online at www.sciencedirect.com

ScienceDirect

Current Opinion in Psychology

Digital privacy in mental healthcare: current issues and recommendations for technology use

Samuel D Lustgarten[1], Yunkyoung L Garrison[2,3], Morgan T Sinnard[1] and Anthony WP Flynn[1]

Mental healthcare providers increasingly use technology for psychotherapy services. This progress enables professionals to communicate, store information, and rely on digital software and hardware. Emails, text messaging, telepsychology/telemental health therapy, electronic medical records, cloud-based storage, apps/applications, and assessments are now available within the provision of services. Of those mentioned, some are directly utilized for psychotherapy while others indirectly aid providers. Whereas professionals previously wrote notes locally, technology has empowered providers to work more efficiently with third-party services and solutions. However, the implementation of these advancements in mental healthcare involves consequences to digital privacy and might increase clients' risk of unintended breaches of confidentiality. This manuscript reviews common technologies, considers the vulnerabilities therein, and proposes suggestions to strengthen privacy.

Addresses
[1] Department of Counseling Psychology, University of Wisconsin-Madison, United States

[2] Department of Psychological and Quantitative Foundations, University of Iowa, Iowa City, United States
[3] Colorado State University Health Network, Fort Collins, United States

Corresponding author:
Lustgarten, Samuel D (sam.lustgarten@gmail.com)

Current Opinion in Psychology 2020, **36**:25–31

This review comes from a themed issue on **Cyberpsychology**

Edited by **Jon D Elhai** and **Dmitri Rozgonjuk**

For a complete overview see the Issue and the Editorial

Available online 6th April 2020

https://doi.org/10.1016/j.copsyc.2020.03.012

Mental healthcare has long held that privacy and confidentiality are primary in the service of clients [e.g., 1,2]. Moreover, psychotherapist-patient privilege has been upheld and supported by the U.S. Supreme Court [3]. Without privacy and confidentiality, therapy may not be effective [4]. However, technological progress has also come with consequences and risks for client privacy. We review current considerations and advancements for various technologies involved in the direct or ancillary provision of services, including emails, text messaging, telepsychology/telemental health therapy, electronic medical records, cloud-based storage, apps/applications, and assessments. We also consider threats and preventative measures to protect client privacy.

Direct use with clients

Email

Mental healthcare professionals use email for scheduling appointments and delivering treatments. The technology enables writers to have more permanence and spontaneity than oral conversations [5]. However, when communicating about Protected Health Information (PHI), email is more vulnerable to unintended breaches/losses than in-person communication [6,7••]. Providers maintain less control over the third-party systems that send and maintain email, which affect their ability to ensure confidentiality [8].

Such a delegation of control poses potential threats to client privacy due to human errors (e.g., sending emails to unintended users), malicious acts, or metadata [9]. Even if the professional minimizes human error, unintended recipients may access and respond to the email [6,5,8]. Lastly, email phishing, which involves hackers posing as someone or an entity to access client data, has been emerging as a common concern for both providers and clients [10•]. According to Elhai and Hall [11], 24.8% of surveyed psychologists reported breaches to their digital mailboxes. Email is also a frequent entryway for spyware and malware, which can be installed to allow malicious users to access the client's PHI [9].

To avoid the threat to client privacy stemming from unsecured emails, Elhai and Frueh [6] recommend mental health professionals use in-transit encryption (i.e., when emails are accessed, read, and sent). Their research showed that 57.4% of their mental health professional research participants used encrypted email services to communicate with their clients [11]. Mental health providers should inform clients about the potential limits of confidentiality in email use [12], along with the risks, benefits, and people who may have access to them.

Text messaging

Text messaging (aka, texting or SMS) is widely utilized across multiple domains of psychotherapy, including psychoeducation [13], appointment reminders [14], treatment

supplementation [15], and delivering interventions [16,17]. Clients increasingly expect to be able to contact providers via text messaging [18]. Although, incorporating text messaging in practice or clinical research may involve novel ethical concerns.

Threats to text messaging privacy can emerge from individual, corporate, and government actors [19]. For instance, phones may be hacked by individuals in an effort to glean private data, corporations may scan and retain text messaging data by default for advertising and marketing purposes, and government agencies may intercept text messages through broad surveillance programs [19]. Elsewhere, it may be difficult to know whether a client is alone when receiving a text or whether they are actually the one texting [20]. Clients may wrongly assume that only providers can access messages, further undermining informed consent [19,20].

To minimize ethical threats, providers should discuss information security directly with clients at treatment onset, and revisit the topic periodically [21]. Notification settings should be adjusted to ensure messages do not appear when the phone is locked or are deidentified [20]. Mental health providers may also consider adopting phones that allow for end-to-end encryption of text messages by default [e.g., Apple's Messages to other iOS users; 19,22,23]. If end-to-end encryption is not possible with native software/apps, providers may choose to adopt alternative messaging apps that offer end-to-end encryption [e.g., Signal; 22,24]. Finally, Drolet [22] advises that providers should be wary of claims of 'Health Insurance Portability and Accountability Act [HIPAA; 25]-compliant' text messaging services (p. 2369). 'HIPAA-compliant' is not a regulated or certified term by the Department of Health and Human Services. Despite claims, providers concerned with compliance are encouraged to de-identify information when transmitted via text message [22].

Telepsychology/telemental health therapy

Numerous terms describe the provision of mental health care via tele/video-conferencing (e.g., televideo or telehealth). For the purposes of this manuscript, we use telepsychology or telemental health therapy (TMHT) as inclusive terms to refer to interactive videoconferencing between mental health providers and clients, ranging from the provision of psychotherapy to medication management. This modality of service delivery has rapidly expanded in recent decades given the ability to mitigate costs and increase access to mental health services [26–28]. TMHT shows particular promise for clients whose access to care is otherwise hampered by situational factors, including rural location, physical health condition, and transportation options [29,30].

Despite the benefits, TMHT services present unique risks to client confidentiality [31•,32]. TMHT sessions may be unintentionally overheard or even maliciously observed by outside parties [33•]. Barnett [31•] recommended that TMHT practitioners 'safeguard' client confidentiality through encryption, HIPAA-compliant software, and protections against adware, malware, and firewalls (p. 424). While Skype or Facetime may be most familiar to clients and providers, more secure and HIPAA-compliant video-conferencing platforms exist [e.g., Doxy.me; 6]. Additionally, TMHT may be affected by the client's location and physical safety.

Shore and colleagues [34] describe best TMHT practices for protecting client privacy, including beginning each session with a thorough verbal assessment of the client's location, the presence of other individuals in the space, and the volume of transmitted audio. Clients may videoconference in their home or workspace, making the private, session content potentially discernible to family members or colleagues. Moreover, some clients may need in-person assistance before engaging in remote therapy [34]. Practitioners should assess the confidentiality of clients in these situations and be transparent about the features and risks during informed consent processes [35].

Apps

'Apps' (mobile applications) are self-contained programs for use on smartphones or tablets [36]. Development and utilization of clinical, treatment-related apps have increased since 2008 [36]. According to the latest estimates, 165,000–325,000 health and wellness apps are available, and over 10,000 apps are designed for mental health [37]. Mental health apps may include reminders and often require clients to record (e.g., written or audio) their symptoms for reviewing the past session or preparing for future sessions [38••,39].

Threats to data privacy via apps are increasing [38••]. Many clients report privacy concerns, which inhibit and discourage use of health-related apps [40,41]. When using apps, various data points are frequently shared with the developers. For instance, behaviors and information (e.g., username and password, contact information, age, gender, location, International Mobile Equipment Identity (IMEI), and phone number) are often monitored by app companies, and some data are sold to third parties [42]. Relatedly, some app privacy policies and terms do not consensually request users for their data [38••].

To address these concerns, providers should acknowledge limits of confidentiality and encourage minimal PHI use and disclosure within apps [43,44•]. In the event of device loss/theft/removal, utilizing remote data wipe tools may be helpful [44•]. Apps are more popular among adolescents than adults. However, younger populations may not understand the implications for privacy and the

permanence of digital footprint; special attention needs to be paid when discussing privacy and consent with adolescents and their parents [45].

Digital assessments

Providers traditionally used paper and pen/pencil for assessments [46••]. One leading assessment company, Pearson Education Inc., began offering digital versions in 2013. For example, the Wechsler Adult Intelligence Scale-Fourth Edition (WAIS-IV), Wechsler Intelligence Scale for Children-Fifth Edition (WISC-V), and Wechsler Memory Scale-Fourth Edition (WMS-IV) are now offered as digital assessments [47]. These digital assessments are conducted with two Apple iPads that connect via Bluetooth (between the two) and then are sent to Pearson's servers for scoring and storage [46••,48].

A paucity of research has been conducted about the legal and ethical risks for digital assessment use. As more assessment companies and mental healthcare providers utilize digital assessments, confidentiality remains a key ethical concern [46••]. Data may be electronically transmitted from the testing/assessment device, leaving providers responsible for maintaining HIPAA regulations [49]. Risk regarding test security and data may also increase in online, digital environments [50].

Providers considering the use of digital assessments should offer informed choices to examinees (or their custodians) and options for tech or paper-based versions (e.g., risks and benefits to using digital assessments). Professionals should consult with assessment specialists for training on differences. Similarly, Apple iPads used for assessments should be designated as sole-purpose devices (i.e., only for digital assessments) to reduce risk of data loss or unintended breaches in confidentiality for devices used in multiple settings. Training programs would likely benefit from incorporating-specific instruction about using technology in the provision of assessments, as well.

Ancillary to client care

General hardware considerations

Regardless of the software/app used, providers must interact with hardware (e.g., smartphones or laptops). For instance, phones are a widespread hardware used for communication between mental healthcare professionals and clients [51,52], which have been employed for decades [53]. However, with the advent and popularization of smartphones and other mobile devices, risk of involuntary disclosure of PHI is greater [44•,54].

Some common phone user behaviors can increase risks of loss or theft, such as leaving their non-password protected device unattended or carrying the device in less secure ways (e.g., handbag or backpack). In fact, 16.8% of security breaches reportedly occurred due to the loss/theft of a smartphone [11]. Elsewhere, while providers may be tempted to utilize new biometric data security measures for securing and unlocking their phones (e.g., fingerprint or facial recognition), a recent U.S. District Court case ruled that law enforcement can legally compel users to unlock their phones via such biometric data [55]. Situations where providers are likely to engage with law enforcement (e.g., international border crossings) present additional threats to client confidentiality of stored text messages. Because prior U.S. case law [e.g., 56] protects individuals from being compelled to reveal number passwords to law enforcement (but not biometric data), providers may consider adopting numerical passwords over biometric data security measures in their professional practice [57].

Mental health professionals are encouraged to verify that the person on the phone is the client [58,59] and should also acknowledge that more confidential means would be via oral and/or written mediums. For example, practitioners may ask each of their clients to complete progress monitoring measures on a shared tablet in the waiting room. Special precautions should be taken to prevent autofill on shared devices to ensure that client data are not inadvertently shared with unauthorized parties [60].

Electronic medical records (EMRs)

An EMR is a computer database that allows healthcare administrators and providers to document information related to patient care [61]. Because of its efficiency and accuracy in documentation relative to paper-based individual documentation, the use of EMRs by government and private medical providers has been on the rise [10•,61]. The National Center for Health Statistics [62] estimates that 85.9% of American doctors in an office setting use electronic health/medical records.

Using an EMR system involves issues related to client privacy, such as how much information is appropriate to place in an EMR, especially when that record is accessible to professionals throughout an organization [61,63•,64,65]. To illustrate, as the other health providers and administrators can access the client care information, each document that mental health professionals create can both intentionally and unintentionally inform all related and unrelated providers and administrators [63•]. Therefore, researchers highlight the importance of fair information practices to reduce any patient digital privacy violations [10•,61,66].

Most informed consent in integrated healthcare settings include limits of confidentiality; however, clients may not always realize what information contained within an EMR is shared with others [63•]. Also, mental health professionals should discuss unique risks of EMRs as well as data storage issues. Risks include system breaches, crashes, and losses of unprotected backups of electronic

PHI [66]. Data storage issues include how their PHI is used, transmitted, stored, and retained in the EMR [67]. Such fair information practices include the least-intrusive, least identifiable, minimally sensitive disclosure to the fewest number of persons as reasonably necessary to achieve the service goals [68].

Cloud-based storage

For mental health practices — large and small — scalability of technology solutions allows for growth of client records without increasing physical footprint or risk to local data. Before the advent and popularization of cloud-storage solutions, providers tended to utilize local hard drives to store document/client notes on their own computers [6]. Over time, cloud storage allowed for greater ease of access to files across devices, locations, and providers. The movement of records to the cloud reduces the risk of fire, flood, natural disaster, and theft/loss associated with local hard drives and/or hardcopy, paper records [6,69].

Various cloud-storage providers market their products as HIPAA compliant [19,70], which may ease the burden on providers to navigate complex regulations and security standards. HIPAA has 18 PHI indicators, some of which include birth dates, addresses, session dates, names, and session notes [71]. By signing business associate agreements (BAAs), psychologists must also maintain privacy and security responsibilities for their own devices.

Storing information online might also challenge providers' awareness of encryption standards, password and device management, and record keeping practices [69,72]. Client records placed in cloud storage increase the risk of unintended breaches in confidentiality and unauthorized access from a distance [9,19,70]. Additionally, various threat actors should be considered, as individuals, organizations, and governments might desire information from clients' records via cloud storage [6,19]. Traditionally underserved populations located in more rural locations and/or with a lower socioeconomic status (SES) also may not have the same technological protections that providers have, which might jeopardize their data stored in the cloud [73]; in these circumstances, other options may be warranted.

Conclusion

In *The Innovators*, biographer Walter Isaacson [74] writes, "Innovation occurs when ripe seeds fall on fertile ground." The 21st century has been highly prosperous for technology companies and their creations. This development has spurred new ideas, thinking, and approaches to the provision of services in the field of psychology.

From rotary phones for calling a client to emails and TMHT, the evolution of practice has been deeply informed by innovation. The use of email, text messaging, TMHT, electronic medical records, cloud-based storage, apps, and digital assessments have all aided providers in their search for efficient and effective care. Moreover, in the face of pandemics or other crises such as COVID-19 (Coronavirus), technology has empowered providers to continue seeing clients from afar when in-person meetings are impossible (e.g., APA's [75] Disaster Mental Health informed consent checklist for telepsychological services).

Simultaneously, mental healthcare providers have been challenged with each advancement in technology use for psychotherapy delivery and general services — from the ethical, legal, and training ramifications of what is implemented. Moving data to digital domains may tax providers' abilities to maintain privacy of PHI. In the face of growing need for technology in practice, providers should consider opportunities for growth and education before use. Providers should engage with relevant literature, attend conferences and continuing education opportunities, and solicit feedback from colleagues, as these actions will likely benefit their work and clients. Ultimately, we implore you to ask, how might this technology affect your clients' privacy? The answers will be crucial for maintaining ethical practice in the future of mental healthcare.

Conflict of interest statement

Nothing declared.

References and recommended reading

Papers of particular interest, published within the period of review, have been highlighted as:

- • of special interest
- •• of outstanding interest

1. American Psychological Association: *Ethical Principles of Psychologists and Code of Conduct*. . (2002, amended effective June 1, 2010, and January 1, 2017) 2017 *https://www.apa.org/ethics/code/*.
2. Fisher MA: **Protecting confidentiality rights: the need for an ethical practice model**. *Am Psychol* 2008, **63**:1-13 http://dx.doi.org/10.1037/0003-066X.63.1.1.
3. *Jaffee v. Redmond*, 518 U.S. 1 (1996).
4. Donner MB, VandeCreek L, Gonsiorek JC, Fisher CB: **Balancing confidentiality: protecting privacy and protecting the public**. *Prof Psychol Res Pract* 2008, **39**:369-376 http://dx.doi.org/10.1037/0735-7028.39.3.369.
5. Moldawsky R, Shah P: **E-mails in a psychiatric practice: why patients send them and how psychiatrists respond**. *Perm J* 2015, **20**:65-69 http://dx.doi.org/10.7812/tpp/15-099.
6. Elhai JD, Frueh BC: **Security of electronic mental health communication and record-keeping in the digital age**. *J Clin Psychiatry* 2016, **77**:262-268 http://dx.doi.org/10.4088/jcp.14r09506.
7. •• Stoll J, Müller JA, Trachsel M: **Ethical issues in online psychotherapy: A narrative reviewFrontiers ina narrative review**. *Psychiatry* 2020, **10**:993 http://dx.doi.org/10.3389/fpsyt.2019.00993

This recent article examined arguments for and against the use of online psychotherapy by conducting a search of major databases. Of

249 samples (e.g., peer-reviewed research, books, chapters), the researchers found 24 ethical arguments for and 32 against the use of online psychotherapy. Privacy and confidentiality was one of the most discussed ethical concerns.

8. Sabin JE, Harland JC: **Professional ethics for digital age psychiatry: boundaries, privacy, and communication**. *Curr Psychiatry Rep* 2017, **19** http://dx.doi.org/10.1007/s11920-017-0815-5.

9. Drummond A, Cromarty P, Battersby M: **Privacy in the digital age: implications for clinical practice**. *Clin Psychol Sci Pract* 2015, **22**:227-237 http://dx.doi.org/10.1111/cpsp.12105.

10. • Jarrett MP: **Cybersecurity—a serious patient care concern**. *JAMA* 2017, **318**:1319 http://dx.doi.org/10.1001/jama.2017.11986
This article highlights the importance of seeing cybersecurity as more than an 'IT problem'. Rather, this article posits that security needs to become everyone's interest. The author suggests physicians and other health providers become engaged in protecting patient/client records by changing passwords, updating software, and advocating for resources at their organization.

11. Elhai JD, Hall BJ: **How secure is mental health providers' electronic patient communication? An empirical investigation**. *Prof Psychol Res Pract* 2015, **46**:444-450 http://dx.doi.org/10.1037/pro0000054.

12. Fantus S, Mishna F: **The ethical and clinical implications of utilizing cybercommunication in face-to-face therapy**. *Smith Coll Stud Soc Work* 2013, **83**:466-480 http://dx.doi.org/10.1080/00377317.2013.833049.

13. Zhao D, Lustria MLA, Hendrickse J: **Systematic review of the information and communication technology features of web- and mobile-based psychoeducational interventions for depression**. *Patient Educ Couns* 2017, **100**:1049-1072 http://dx.doi.org/10.1016/j.pec.2017.01.004.

14. Clough B, Casey LM: **Using SMS reminders in psychology clinics: a cautionary tale**. *Behav Cogn Psychother* 2014, **42**:257-268 http://dx.doi.org/10.1017/S1352465813001173.

15. Aguilera A, Bruehlman-Senecal E, Demasi O, Avila P: **Automated text messaging as an adjunct to cognitive behavioral therapy for depression: a clinical trial**. *J Med Internet Res* 2017, **19**:e148 http://dx.doi.org/10.2196/jmir.6914.

16. Rathbone AL, Presscot J: **The use of mobile apps and SMS messaging as physical and mental health interventions: systematic review**. *J Med Internet Res* 2017, **19**:e295 http://dx.doi.org/10.2196/jmir.7740.

17. Wilhelm S, Weingarden H, Ladis I, Braddick V, Shin J, Jacobson NC: **Cognitive-behavioral therapy in the digital age: presidential address**. *Behav Ther* 2020, **51**:1-14 http://dx.doi.org/10.1016/j.beth.2019.08.001.

18. Maheu MM, Pulier ML, McMenamin JP, Posen L: **Future of telepsychology, telehealth, and various technologies in psychological research and practice**. *Prof Psychol Res Pract* 2012, **43**:613-621 http://dx.doi.org/10.1037/a0029458.

19. Lustgarten SD: **Emerging ethical threats to client privacy in cloud communication and data storage**. *Prof Psychol Res Pract* 2015, **46**:154-160 http://dx.doi.org/10.1037/pro0000018.

20. Sude ME: **Text messaging and private practice: ethical challenges and guidelines for developing personal best practices**. *J Ment Health Couns* 2013, **35**:211-227 http://dx.doi.org/10.17744/mehc.35.3.q37l2236up62l713.

21. Pham AV, Goforth AN, Segool N, Newman S: **Challenges of emerging technology: social networking and texting in pediatric neuropsychology practice**. *J Pediatr Neuropsychol* 2018, **4**:16-26 http://dx.doi.org/10.1007/s40817-017-0038-z.

22. Drolet BC: **Text messaging and protected health information: what is permitted?** *JAMA* 2017, **317**:2369-2370 http://dx.doi.org/10.1001/jama.2017.5646.

23. Hassinen M, Laitinen P: **End-to-end encryption for SMS messages in the health care domain**. *Stud Health Technol Inform* 2005, **116**:316-321.

24. Ermoshina K, Musiani F, Halpin H: **End-to-end encrypted messaging protocols: an overview**. *Presented at the 3rd International Conference on Internet Science; Florence, Italy, Sep 2015, New York, NY: Springer: 2016*.

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

26. American Psychological Association: **Guidelines for the practice of telepsychology**. *Am Psychol* 2013, **68**:791-800 http://dx.doi.org/10.1037/a0035001.

27. Mehrotra A, Jena AB, Busch AB, Souza J, Uscher-Pines L, Landon BE: **Utilization of telemedicine among rural Medicare beneficiaries**. *J Am Med Assoc* 2016, **315**:2015-2016 http://dx.doi.org/10.1001/jama.2016.2186.

28. Mehrotra A, Huskamp HA, Souza J, Uscher-Pines L, Rose S, Landon BE *et al.*: **Rapid growth in mental health telemedicine use among rural Medicare beneficiaries, wide variation across states**. *Health Aff* 2017, **36**:909-917 http://dx.doi.org/10.1377/hlthaff.2016.1461.

29. Guzman D, Ann-Yi S, Bruera E, Wu J, Williams JL, Najera J *et al.*: **Enhancing palliative care patient access to psychological counseling through outreach telehealth services**. *Psycho-Oncology* 2020, **29**:132-138 http://dx.doi.org/10.1002/pon.5270.

30. U.S. Department of Veterans Affairs: *VA Mental Health Care Fact Sheet*. . [Fact sheet]. Retrieved from 2016 *https://www.va.gov/opa/publications/factsheets/April-2016-Mental-Health-Fact-Sheet.pdf*.

31. • Barnett JE: **The ethical practice of psychotherapy: Clearly within our reachPsychotherapy564clearly within our reach**. *Psychotherapy* 2019, **56**:431-440 http://dx.doi.org/10.1037/pst0000272
The author spotlights the absence of technology considerations within APA's (2017) ethical sections and standards, noting inclusion of distance-based care within the American Counseling Association's code. Recommendations are provided to psychologists interested in implementing technology in practice, such as acquiring competence, discussing usage in informed consent processes, and researching the empirical support for apps.

32. Lustgarten SD, Colbow AJ: **Ethical concerns for telemental health therapy amidst governmental surveillance**. *Am Psychol* 2017, **72**:159-170 http://dx.doi.org/10.1037/a0040321.

33. • Wrape ER, McGinn MM: **Clinical and ethical considerations for delivering couple and family therapy via telehealth**. *J Marital Fam Ther* 2019, **45**:296-308 http://dx.doi.org/10.1111/jmft.12319
Various articles discuss the considerations related to technology use with individuals, Wrape and McGinn highlight unique ethical concerns within couples and family therapy. The authors report that couples work can limit privacy (e.g., not being able to isolate sound as well when engaged in telemental therapy), detract from therapist confidence in feedback processes, interruptions in local environment, and may involve greater risk to safety when domestic violence is present.

34. Shore JH, Yellowlees P, Caudill R, Johnston B, Turvey C, Mishkind M *et al.*: **Best practices in videoconferencing-based telemental health**. *Telemed E-Health* 2018, **24**:827-832 http://dx.doi.org/10.1089/tmj.2018.0237.

35. Chaet D, Clearfield R, Sabin JE, Skimming K: **Ethical practice in telehealth and telemedicine**. *J Gen Intern Med* 2017, **32**:1136-1140.

36. Fairburn CG, Rothwell ER: **Apps and eating disorders: a systematic clinical appraisal**. *Int J Eat Disord* 2015, **48**:1038-1046 http://dx.doi.org/10.1002/eat.22398.

37. Carlo AD, Hosseini Ghomi R, Renn BN, Areán PA: **By the numbers: ratings and utilization of behavioral health mobile applications**. *NPJ Digit Med* 2019, **2** http://dx.doi.org/10.1038/s41746-019-0129-6.

38. •• Parker L, Halter V, Karliychuk T, Grundy Q: **How private is your mental health app data? An empirical study of mental health**

app privacy policies and practices. *Int J Law Psychiatry* 2019, **64**:198-204 http://dx.doi.org/10.1016/j.ijlp.2019.04.002
These authors collected and analyzed 61 medical and mental health apps. This research provides a comprehensive understanding of the ecosystem for mental health, highlighting that most apps tend to focus on anxiety/panic (56%) and depression/mood (26%). In 2018, of the 44 apps on the Google Play store, they requested an average 7.6 permissions (e.g., device data, record audio, read/write storage, text messages, and contact lists). The authors note that improvements in privacy and permissions have occurred over the years, but many companies remain interested in data harvesting.

39. Torous J, Nicholas J, Larsen ME, Firth J, Christensen H: **Clinical review of user engagement with mental health smartphone apps: evidence, theory and improvements**. *Evid Based Ment Health* 2018, **21**:116-119 http://dx.doi.org/10.1136/eb-2018-102891.

40. Martínez-Pérez B, de la Torre-Díez I, López-Coronado M: **Privacy and security in mobile health apps: a review and recommendations**. *J Med Syst* 2015, **39**:1-8 http://dx.doi.org/10.1007/s10916-014-0181-3.

41. VonHoltz LAH, Hypolite KA, Carr BG, Shofer FS, Winston FK, Hanson CW, Merchant RM: **Use of mobile apps: a patient-centered approach**. *Acad Emerg Med* 2015, **22**:765-768 http://dx.doi.org/10.1111/acem.12675.

42. Martinez-Martin N, Kreitmair K: **Ethical issues for direct-to-consumer digital psychotherapy apps: addressing accountability, data protection, and consent**. *JMIR Ment Health* 2018, **5**:e32 http://dx.doi.org/10.2196/mental.9423.

43. Jones N, Moffitt M: **Ethical guidelines for mobile app development within health and mental health fields**. *Prof Psychol Res Pract* 2016, **47**:155-162 http://dx.doi.org/10.1037/pro0000069.

44. • Karcher NR, Presser NR: **Ethical and legal issues addressing the use of mobile health (mHealth) as an adjunct to psychotherapy**. *Ethics Behav* 2018, **28**:1-22 http://dx.doi.org/10.1080/10508422.2016.1229187
This article emphasizes the privacy and confidentiality concerns when providers use text messaging and apps for psychotherapy. The authors write that responsibility remains on providers for ensuring their recommendations meet ethical standards. Privacy and security breaches across domains – software and hardware –– are acknowledged, with particular interest on tablets, smartwatches, and other portable devices that might be seen by others in a less private setting (e.g., home or at work).

45. Sussman N, DeJong SM: **Ethical considerations for mental health clinicians working with adolescents in the digital age**. *Curr Psychiatry Rep* 2018, **20** http://dx.doi.org/10.1007/s11920-018-0974-z.

46. •• Jellins L: **Assessment in the digital age: An overview of online tools and considerations for school psychologists and school counsellors**. *J Psychol Couns Sch* 2015, **25**:116-125 http://dx.doi.org/10.1017/jgc.2015.8
Although older than two years, Jellins provides insight on current growth in the use of digital assessments, and is one of few peer-reviewed articles to highlight this new technology. The article acknowledges a study involving school psychologists, as they incorporate more technology in their schools. Initial reports suggested teachers involved in study appreciated the efficiency and productivity. Jellins noted that those involved in the study were cautious regarding data sharing practices, and worked to minimize (e.g., use initials) personal information shared with third-party services.

47. Pearson Education Inc: *Q-interactive: Library*. . Retrieved February 23, 2020, from 2020 *https://www.pearsonassessments.com/professional-assessments/digital-solutions/q-interactive/test-components.html?tab=library*.

48. Pearson Education Inc: *Q-interactive: System Requirements*. . Retrieved February 23, 2020, from 2020 *https://www.pearsonassessments.com/professional-assessments/digital-solutions/q-interactive/test-components.html?tab=system-requirements*.

49. Lustgarten SD, Elhai JD: **Technology use in mental health practice and research: legal and ethical risks**. *Clin Psychol Sci Pract* 2018, **25**:e12234 http://dx.doi.org/10.1111/cpsp.12234.

50. Naglieri JA, Drasgow F, Schmit M, Handler L, Prifitera A, Margolis A, Velasquez R: **Psychological testing on the Internet: new problems, old issues**. *Am Psychol* 2004, **59**:150-162 http://dx.doi.org/10.1037/0003-066X.59.3.150.

51. Pennington M, Patton R, Ray A, Katafiasz H: **A brief report on the ethical and legal guides for technology use in marriage and family therapy**. *J Marital Fam Ther* 2017, **43**:733-742 http://dx.doi.org/10.1111/jmft.12232.

52. Sokol DK, Car J: **Patient confidentiality and telephone consultations: time for a password**. *J Med Ethics* 2006, **32**:688-689 http://dx.doi.org/10.1136/jme.2005.014415.

53. Campbell LF, Norcross JC: **Do you see what we see? Psychology's response to technology in mental health**. *Clin Psychol Sci Pract* 2018, **25**:e12237 http://dx.doi.org/10.1111/cpsp.12237.

54. Taube DO: **Portable digital devices: meeting challenges to psychotherapeutic privacy**. *Ethics Behav* 2013, **23**:81-97 http://dx.doi.org/10.1080/10508422.2012.722502.

55. *United States v. Barrera*, 19 CR 439, (N. D. Ill, 2019).

56. *Pennsylvania v. Davis*, JU-42-2019, (S. C. Pen, 2019).

57. Paul G, Irvine J: **Fingerprint authentication is here but are we ready for what it brings?** *IEEE Consumer Electronics Magazine*. 2015 https://pdfs.semanticscholar.org/2b17/8cbc690d4f39bc967670d2c20519294.pdf.

58. Brenes GA, Ingram CW, Danhauer SC: **Benefits and challenges of conducting psychotherapy by telephone**. *Prof Psychol Res Pract* 2011, **42**:543-549 http://dx.doi.org/10.1037/a0026135.

59. Koocher GP: **Twenty-first century ethical challenges for psychology**. *Am Psychol* 2007, **62**:375-384 http://dx.doi.org/10.1037/0003-066x.62.5.375.

60. Knijnenburg BP, Kobsa A, Jin H: **Counteracting the negative effect of form auto-completion on the privacy calculus**. In *Proceedings of the 34th International Conference on Information Systems (ICIS 2013)*; *Milan, Italy: 2013*.

61. Steinfeld BI, Keyes JA: **Electronic medical records in a multidisciplinary health care setting: a clinical perspective**. *Prof Psychol Res Pract* 2011, **42**:426-432 http://dx.doi.org/10.1037/a0025674.

62. National Center for Health Statistics: *Table. Percentage of Office-Based Physicians Using Any Electronic Health Record (EHR)/Electronic Medical Record (EMR) System and Physicians That Have a Certified EHR/EMR System, by U.S. State: National Electronic Health Records Survey, 2017*. 2017 https://www.cdc.gov/nchs/data/nehrs/2017_NEHRS_Web_Table_EHR_State.pdf.

63. • Magruder JA, Adams BS, Pohto P, Smith TL: **Clinicians' experiences of transition to electronic health records**. *J Coll Couns* 2018, **21**:210-223 http://dx.doi.org/10.1002/jocc.12104
This study examined the experiences of five clinicians using electronic health records. Researchers utilized a qualitative approach called grounded theory to gather and analyze the experiences. Change, perceived control, and efficiency were the three major themes the researchers found. Most participants acknowledged resistance to change, but many noted efficiency gains –– with some glitches along the way.

64. Shenoy A, Appel JM: **Safeguarding confidentiality in electronic health records**. *Cambridge Q Healthc Ethics* 2017, **26**:337-341 http://dx.doi.org/10.1017/S0963180116000931.

65. Yüksel B, Küpçü A, Özkasap Ö: **Research issues for privacy and security of electronic health services**. *Future Gener Comput Syst* 2017, **68**:1-13 http://dx.doi.org/10.1016/j.future.2016.08.011.

66. Holmes CM, Reid CA: **Ethics in telerehabilitation: looking ahead**. *J Appl Rehabil Couns* 2018, **49**:14-23 http://dx.doi.org/10.1891/0047-2220.49.2.14.

67. Wilkinson T, Reinhardt R: **Technology in counselor education: HIPAA and HITECH as best practice**. *Prof Couns* 2015, **5**:407-418 http://dx.doi.org/10.15241/tw.5.3.407.

68. DeJong SM: **Professionalism and technology: competencies across the tele-behavioral health and e-behavioral health spectrum**. *Acad Psychiatry* 2018, **42**:800-807 http://dx.doi.org/10.1007/s40596-018-0947-x.

69. Rigg T: **The ethical considerations of storing client information online**. *Prof Psychol Res Pract* 2018, **49**:332-335 http://dx.doi.org/10.1037/pro0000217.

70. Zur O: **Telepsychology or telementalhealth in the digital age: the future is here**. *Calif School Psychol* 2012, **45**:13-15.

71. University of California Berkeley: *HIPAA PHI: List of 18 Identifiers and Definition of PHI*. 2020 https://cphs.berkeley.edu/hipaa/hipaa18.html.

72. Klein CA: **Cloudy confidentiality: clinical and legal implications of cloud computing in health care**. *J Am Acad Psychiatry Law* 2011, **39**:571-578.

73. Cooper SE, Campbell LF, Barnwell SS: **Telepsychology: a primer for counseling psychologists**. *Couns Psychol* 2019, **47**:1074-1114 http://dx.doi.org/10.1177/0011000019895276.

74. Isaacson W: *The Innovators: How a Group of Hackers, Geniuses, and Geeks Created the Digital Revolution*. Simon & Schuster; 2014.

75. American Psychological Association: *Informed Consent Checklist for Telepsychological Services*. 2020 https://www.apa.org/practice/programs/dmhi/research-information/informed-consent-checklist.