Security of Electronic Mental Health Communication and Record-Keeping in the Digital Age

Jon D. Elhai, PhD, and B. Christopher Frueh, PhD

ABSTRACT

The mental health field has seen a trend in recent years of the increased use of information technology, including mobile phones, tablets, and laptop computers, to facilitate clinical treatment delivery to individual patients and for record keeping. However, little attention has been paid to ensuring that electronic communication with patients is private and secure. This is despite potentially deleterious consequences of a data breach, which are reported in the news media very frequently in modern times. In this article, we present typical security concerns associated with using technology in clinical services or research. We also discuss enhancing the privacy and security of electronic communication with clinical patients and research participants. We offer practical, easy-to-use software application solutions for clinicians and researchers to secure patient communication and records. We discuss such issues as using encrypted wireless networks, secure e-mail, encrypted messaging and videoconferencing, privacy on social networks, and others.

J Clin Psychiatry 2016;77(2):262–268
dx.doi.org/10.4088/JCP.14r09506

Submitted: September 12, 2014; accepted January 22, 2015.
Online first: August 18, 2015.

Corresponding author: Jon D. Elhai, PhD, Department of Psychology, University of Toledo, Mail Stop #948, 2801 W Bancroft St, Toledo, OH 43606-3390 (for electronic correspondence, visit www.jon-elhai.com).

The mental health field has seen a trend in recent years of increased use of information technology and electronic devices for clinical assessment and treatment of individual patients.[1] Several researchers argue that such modalities, including e-mail, instant messaging, software application ("app") use, videoconferencing, and others, can assist in the logistics of scheduling and maintaining appointments,[2] as well as in facilitating psychological and psychiatric treatment.[1,3] Further, patients report being interested in using technology in treatment.[4] Despite the sensitivity and stigma associated with mental health disorders and treatment,[5,6] surprisingly little has been written about issues of privacy and security of electronic communication in mental health settings.[7]

In this article, we discuss common weaknesses in privacy and security typically seen in the use of electronic health communication and record keeping and offer practical, easy-to-implement solutions for overcoming these limitations using better privacy and security solutions. The risks to providers of the loss or theft of patient data can include Health Insurance Portability and Accountability Act (HIPAA) violations, licensing sanctions, and civil lawsuits.[8] These risks are very real as the health industry becomes more and more paperless and interconnected online.[9] In fact, clinicians are increasingly using mobile devices to access patient records.[10] Mental health providers report incidents of compromised electronic privacy, such as unauthorized forwarding of patient e-mails,[11] as well as lack of attention to social media privacy settings, resulting in social media oversharing that can be seen by patients.[12]

Our hope is that clinicians and researchers maintain more rigorous privacy and security practices, such as those discussed in this article, in the delivery of mental health care and communication with patients. This issue is crucial in ensuring that patient anonymity and electronic data are kept between the patient, provider, and insurance company and protected from access by unauthorized parties.

We begin with a caveat regarding the likelihood of compromised electronic privacy or security. Without the consumer's using enhanced security procedures, compromising e-mail and instant messaging is not uncommon and not difficult for an unauthorized party or bad actor (ie, a "hacker") to do.[13,14,a] In fact, about half of all Americans were hacked in the past year.[15] The focus of our article is primarily on providing concrete suggestions for preventing this kind of data compromise.

In addition, modern law enforcement and the intelligence community (eg, National Security Agency [NSA]) routinely compromise individuals' electronic communication and data, social media accounts, and physical "smartphones," as recently reported in the Edward Snowden leaks.[16,17] For practical reasons, in this article we focus primarily on preventing individual hacker compromises of such communication. However, we can identify at least 2 reasons to be

[a] We cite several reputable technology websites and blogs and general news sources throughout this article. The technology sites may be unfamiliar to the mental health audience of this journal. However, in the technology field, these blogs are well respected.

Clinical Points

- Common practices for use of information technology in the digital age are not adequate for secure, HIPAA-compliant communication and record keeping, and mental health clinicians should ensure that they are using secure methods of electronic communication with their patients.
- Reviewing and adhering to the suggestions provided in this article for securing one's electronic communication will help maintain confidentiality of patient communication.

cognizant of NSA-style surveillance in the context of clinical treatment: (1) classically suspicious/paranoid or seriously mentally ill patients may be especially concerned about this issue, which can thus impact treatment, and (2) we wonder how long it will take before a nonsecure instant message or e-mail from a treatment provider that establishes a suicide contract is flagged by government surveillance, resulting in law enforcement's interviewing the provider and/or patient about this commonly accepted treatment practice.

We now discuss weaknesses in the use of specific common electronic communication and preventive precautions to enhance privacy and security. In suggesting software solutions, we offer no- or low-cost solutions when possible, especially because some of these solutions require use by the patient in addition to the provider. Additionally, because some technology trends come and go fairly quickly, and many startup companies do not last, we have attempted to focus on high-quality solutions from companies that have garnered generous media attention and venture capital and thus have a likelihood of enduring. When possible, we provide references (typically website links) for step-by-step instructions in implementing these solutions. For non–technologically savvy users, this discussion will quite likely be unfamiliar, although we have attempted to present the information in very basic, nontechnical terms. Even for advanced, technologically savvy users, a good deal of this information will quite likely be unfamiliar. We also provide Table 1, which gives brief information on how long each solution takes to set up (estimated) and how difficult each solution is to set up and use.

Network

Hard-wired (ie, nonwireless) networks are generally safe and not conducive to interception by hackers as long as the consumer is using a firewall. Most Internet routers have firewalls built into the firmware; modern Apple and Windows computers have a firewall option built into their operating systems that can be selected in the preferences or system settings; for a brief tutorial, see Gordon.[18] Enabling the firewall can prevent unwanted Internet traffic from intruding on one's network or electronic devices and thus can prevent theft of patient data.

Wireless networks can pose a greater threat to privacy and security. Thus, private wireless networks (eg, at a provider's home) should be password-protected using Wi-Fi Protected Access (WPA) encryption rather than the extremely easy to crack Wired Equivalent Privacy (WEP) encryption; for a step-by-step tutorial, see Purdy.[19] In addition, many hospitals and private mental health practices offer public wireless Internet access to their staff and patients. On such public wireless networks, it is quite easy and common for hackers to intercept network data, resulting in unauthorized viewing or theft of data.[20] Thus, private data in patient records could be retrieved by unauthorized parties.

To avoid such breaches on public wireless networks, we offer several suggestions. First, communicate only on encrypted websites. That is, when using a public wireless network, ensure that any data transmission is done on websites that have the "https" prefix in their Web address rather than the "http" prefix. The *s* in "https" indicates that the site uses encrypted data transfers (ie, the standard used in bank transactions, for example) and thus is secure. Some websites do not offer "https" encryption on their site as default, but offer the option of using "https" in the user's account settings. For an easy and convenient solution, we recommend the free HTTPS Everywhere computer software, which assists by automatically activating an encrypted connection on websites that support encrypted communication. This software, developed by the Tor Project and Electronic Frontier Foundation (EFF), is a Web browser extension for Google Chrome and Mozilla Firefox Web browsers and ensures that the user's connection is always encrypted when visiting these websites. We routinely use this service and find it helpful and secure, and it can be acquired at www.eff.org/https-everywhere.

A more secure option on public networks, especially if using websites for communication that do not support encryption, is to use a virtual private network (VPN). Using a VPN, the user is essentially tunneling his or her Internet traffic out of the public wireless network to an outside server (perhaps in a different city or country), making it impossible for individuals on the public wireless network to intercept the user's communication. There are plenty of VPN options to choose from, some of which are discussed elsewhere.[21] Free VPNs with limited features are also available. We have used the Cloak VPN service, which we like because it is easy to use, typically has fast performance, is available on computers and mobile devices, and is inexpensive (currently as little as $3 per month). We believe that most non–technologically savvy users would find this service quite easy to use. Cloak can be acquired at www.getcloak.com.[b]

[b] One final note on VPNs relates to the use of The Onion Router (Tor). Tor involves tunneling communication through several different servers in multiple locations across the world, for increased anonymity and security. Originally developed to protect government communication, Tor is now often used, for example, by activists in dangerous parts of the world to remain anonymous and thus safe from physical retaliation and by journalists to protect their stories and sources. The Tor browser is available for free on computers and mobile devices; however, it is probably unnecessary solely for protecting patient data. Also, because of the sequential routing, Internet speeds are typically slow as a result. Tor is available from www.torproject.org.

Table 1. Setup and Use Characteristics of Security Solutions

Solution	Estimated Time to Setup/Install	Difficulty to Install/Implement	Difficulty to Use
Running a system software update	5 min to set up/up to an hour (or more) to run passively in background	Easy	NA
Setting up WPA encryption on a home router	15 min	Easy to medium	Easy
HTTPS Everywhere	5 min	Easy	Easy
Cloak	5 min	Easy to medium	Easy
Tor	5 min	Medium	Medium
Riseup	5 min (web-based e-mail)/10 min (basic set up on an e-mail software package)	Easy (web-based e-mail) to medium (e-mail software package)	Easy
Virtru	5 min	Easy	Easy
iPGMail	30–45 min	Difficult	Medium
Wickr	5 min	Easy	Easy
Burner	5 min	Easy	Easy
Microsoft Security Essentials	5 min	Easy	Easy
ClamXav	5 min	Easy	Easy
FileVault	10 min to set up/several hours to run passively in background while encrypting for first time	Easy	NA
Setting a firmware password	5 min	Easy	NA
Setting a BIOS password	5 min	Easy	NA
Dropbox	5 min	Easy	Easy
Two-factor authentication for a web account	5 min	Easy	Medium
Configuring Facebook security/privacy settings	30 min	Medium	NA

Abbreviations: NA = not applicable, WPA = Wi-Fi Protected Access.

Videoconferencing

Videoconferencing has been used with increasing frequency as a delivery mode for treating mental health patients,[22,23] providing an alternative to in-person, face-to-face treatment. High-end videoconferencing hardware and software by such companies as Polycom and Cisco generally offer advanced security features. However, most people tend to use free services such as Google Hangouts, Skype, and FaceTime to videoconference,[24] which tend not to offer good security.[25] In addition to videoconferencing over a VPN, we suggest alternative, more secure videoconferencing clients. There are third-party vendors who can complement free services such as Skype, to increase their security. AkCode Summit is one service recently used by some VA Medical Centers, although it is relatively expensive (www.akcode.com). Doxy.me provides a similar service, and it is HIPAA compliant and free to use (www.doxy.me/telemedicine). Finally, Jitsi is a service we recently started using and find helpful (http://jitsi.org).

E-Mail

E-mail is frequently used by mental health providers in communicating with patients.[12] E-mail is not necessarily a secure platform for communication. Thus, data from scheduling appointments or e-mail communication to check in and monitor symptoms can be accessible by hackers. Web-based e-mail can be secured by using an encrypted "https" connection, as detailed above. Most popular e-mail providers, such as Gmail, Yahoo, and Hotmail, offer "https" encryption by default or as an optional feature in an account user's settings (and/or by using HTTPS Everywhere). However, these services are subsidized by targeted advertisements, and thus some privacy is most likely sacrificed. We often use and recommend the free, encrypted Riseup service (for computers and mobile devices), offered by a nonprofit organization that advocates for digital security and takes privacy seriously (www.riseup.net).

One limitation of e-mail encryption is that it is only as secure as the weakest link in an e-mail exchange. So if a mental health provider using an encrypted e-mail connection is communicating with a patient who is not using an encrypted e-mail connection, then e-mail on the patient's end will not be secure. For more enhanced security, then, we would suggest using end-to-end e-mail encryption. For example, both the patient and provider could use the Riseup service to provide end-to-end encryption on both sides of the communication.[c]

Instant Messaging

Many mental health providers have begun to use instant messaging (eg, texting or chatting) with their patients.[1] For a discussion of the merits and potential problems that can arise from messaging with patients, see DeJong and Gorrindo.[28]

From a security perspective, there are 2 primary concerns with messaging patients. First (without extra precautions discussed below), messaging may not be secure, and messages can be intercepted by unauthorized parties.[13] Second, many

[c] End-to-end encryption with a service such as Riseup works for Web-based e-mail. If Riseup is used on a smartphone or computer with a third-party e-mail client (eg, Outlook, Apple Mail) to communicate, however, the third-party client may not be encrypted. There are advanced, state-of-the-art methods known as Pretty Good Privacy (PGP) for securing e-mail on a computer e-mail client, but they are not easy to set up and thus not for the average user. Instructions for the truly ambitious, advanced user can be found elsewhere.[26] Somewhat easier to use (but still a bit complicated) is the iPGMail mobile app, which uses PGP (www.ipgmail.com). Easy-to-use apps that offer end-to-end encryption have only very recently begun appearing. Some shut their services down in 2013, apparently in response to government intelligence agencies requiring their e-mail server access.[27] We have used Virtru (for computers and mobile devices), which we recommend (www.virtru.com).

individuals do not password-protect their mobile phones, even though password protection and/or encryption are available features on most modern smartphones. Thus, sensitive communication (ie, messages, voice mails) with a mental health patient could be easily discoverable if the mental health provider's phone is lost, stolen, or even left unattended.[8]

We suggest first that mental health providers password-protect their phones (using the phone's security settings). In fact, the newest Apple iPhone/iPad operating system (iOS 8) is encrypted so securely that Apple is not able to access one's phone data, even with a valid search warrant; Google's Android operating system will follow similarly soon.[29] Second, we suggest that providers not use standard Short Message Service (SMS) or instant messaging with patients. Instead, encrypted, self-destructing messaging should be used for patient communication—by both the provider and patient. Some of these messaging applications use end-to-end encryption to keep messages secure. Messages are automatically removed from one's phone (and the company's servers) after a predefined (or user-customized) period of time. Several of these applications are discussed elsewhere.[30] An advantage of some of these applications is that they include a verification process to ensure that the 2 people communicating are each speaking to the intended person.[31] We often use the free Wickr application, which is easy to use, is available on mobile devices, and can be obtained from www.wickr.com. Other encrypted messaging applications are discussed elsewhere.[32] The EFF has a useful audit of many secure messaging applications to assess how they stack up to one another.[33]

Phone Calls

One problem often faced by mental health providers, even those willing to message their patients, is the preference not to provide the patient with the provider's personal mobile phone number. A common scenario is one in which the provider receives a page or call from his or her answering service to return a patient's phone call on a weekend or evening. The provider is faced with the option of either (1) returning the patient's call from the provider's cell or home phone (and inadvertently allowing the patient to see the phone number on the patient's Caller ID display; this can be risky if the patient later makes frequent, unwanted calls to that number) or (2) having to inconveniently find a public phone from which to return the call.

We suggest using a service that allows placement of cell phone calls and instant messages without revealing one's cell phone number. We sometimes use and recommend the Burner app for mobile devices for this purpose. With Burner, users can choose temporary or permanent cell phone numbers to use from within the mobile app on their phone. Burner can be customized to allow the patient to see only the provider's Burner number when the provider calls/messages the patient, while returned calls/messages from the patient are anonymously forwarded to the provider's real cell phone number. Burner is free to download, inexpensive to subscribe to (as little as $2 to $3 per month), and can be acquired from www.burnerapp.com.

Computer Use

Mental health providers keep patient data on their computers and may communicate with patients using their computers (eg, e-mail). It is therefore important to keep clinic computers secure.

We recommend several security precautions, to begin with, in securing one's computer. First, we recommend that users update their computer operating system and apps when prompted to do so. Updates often plug security vulnerabilities that are exploited by hackers. Windows and Apple operating systems are now configured to provide automatic update prompting as the default. Second, all users should have an antivirus app with weekly scanning for viruses and malware; a schedule can be set up in the software to run automatically at a specified schedule, such as weekly. Computers that are infected by viruses or malware can be controlled and monitored by unauthorized parties. More information on the dangers of viruses and malware is posted elsewhere.[34] We have used and recommend the free Microsoft Security Essentials antivirus/antimalware software for Windows (http://windows.microsoft.com/en-us/windows/security-essentials-download). For Apple computers, we have used and recommend the free ClamXav software (http://www.clamxav.com). Additional antivirus and antimalware software is discussed in Henry.[34]

Third, we recommend encrypting computers that contain patient data and/or communication. Merely password-protecting a computer is inadequate, as it is quite easy to bypass a computer's system password.[35] For Apple computers, we have used and recommend the built-in FileVault software. For Windows computers, Gordon[35] discusses encryption software apps for Windows (however, we should note that his article discusses the TrueCrypt encryption software, which has since been found insecure and is not recommended). We also recommend using such software to encrypt the contents of flash drives that providers may use to transport data among providers or from computer to computer. Flash drives are small enough to be easily overlooked, lost, or stolen.

Fourth, in addition to encrypting one's computer, we recommend setting a firmware or BIOS password on computers. Without a firmware password, an unauthorized user can enter safe/recovery mode on a computer or boot the computer from a flash drive or CD/DVD in order to access the computer's contents. We recommend setting a firmware password on Apple computers[36] and a BIOS password on Windows computers.[37]

Finally, we recommend properly disposing of computers when they are ready for retirement. Proper disposal would involve more than simply erasing the contents of the computer prior to disposing or recycling; a typical reformat does not fully wipe all contents. Instead, a secure erase is recommended, using software discussed elsewhere.[38] Alternatively, one may drive a nail or screw through the computer's hard drive, rendering it inoperable.

Backup

We discussed enhancing computer security in the previous section. Because computers can crash and can be stolen or lost, it is also important to properly back up their contents. This is especially relevant for mental health clinicians who use their computers to write progress notes and reports and to schedule appointments. Losing patient records without the ability to retrieve them is a HIPAA compliance issue and inadequate for continuity of care.

Medium to large health care networks, hospitals, and clinics typically have information technology departments that keep computers on their networks backed up. Independent clinicians would greatly benefit from a computer backup strategy as well.

Before cloud storage became popular in recent years, routinely backing up a computer to an external hard drive or local computer server was a sensible solution. However, this strategy required the user to remember to initiate a backup. It also was risky if damage or theft happened to both one's computer and backup hard drive at the same location. Currently, cloud storage is a convenient set-up-and-forget-it strategy. One can use such a service to continually and incrementally keep a computer backed up automatically whenever the computer has an Internet connection. Several cloud storage services, free as well as paid, are available to consumers and businesses, such as Google Drive and iCloud. We use the paid version of Dropbox because it is relatively inexpensive ($10 per month), holds a very generous amount of computer data (1 terabyte), allows users to back up and sync their data with many different kinds of devices, allows sharing and collaboration, is very commonly integrated into other apps, and uses encryption to transmit data. Other services are discussed elsewhere.[39]

Social Networks

Many mental health providers use social media networks, either for personal accounts or for promoting their clinical practices. If the provider wants to limit sharing of information in his or her personal account (from patients or prospective patients), most social networks have numerous hurdles to jump over in order to properly secure an account. Typical preferences for enhancing privacy most likely involve protecting from the public the following types of data: family photos and videos, posts and status updates, contact information, and personal profile information. Such data can be limited to only preapproved friends/followers. Koh et al[12] recommend occasionally reviewing security and privacy settings on social networks; we suggest also revisiting these settings when the social network announces changes to their privacy policy or settings. Gordon[40] presents a fairly comprehensive guide to securing one's Facebook account, for example.

Two-Factor Authentication

Finally, although it is perhaps for the advanced user, we should mention 2-factor authentication. This free security strategy offered by several major Web sites provides protection against breaching of one's Internet account by a hacker. Two-factor authentication offers the user the ability to require a special code to be entered when logging into an Internet account, in addition to entering one's username and password.[41] When an attempt is made to log in, the code is sent to one's cell phone, to one's e-mail address, or within a special authentication smartphone app. Thus, 2 methods are required in order to access the Internet account, the username/password combination and access to an authentication code, thereby making hacking substantially more difficult.

CASE STUDY

We have presented numerous solutions to secure electronic communication for mental health providers. This information can seem distant or irrelevant in an abstract sense. Therefore, we present a brief, fictional case study of how these security enhancements can be practically used on a day-to-day basis by a mental health provider by providing a typical day of use of such technology.

Eric is a 45-year-old clinical psychologist. He is employed in a shared private practice with 3 other mental health professionals. He practices in Charleston, South Carolina.

It is a Tuesday morning, and Eric arrives at his office at about 9:15 AM. *After getting settled, he starts up his Apple MacBook Pro laptop; it is encrypted with Apple's FileVault and has a firmware password that he set. Occasionally, Eric takes his laptop home to write assessment reports. Because it is encrypted, he does not worry about patient data being exposed if his laptop is stolen. All of his files are backed up and synced on Dropbox, so he does not worry about losing his work. His only worry is the cost of replacing the laptop if stolen.*

Eric's practice has wired Ethernet and wireless Internet, with their router protected with WPA2 encryption using a strong password that only clinic staff and providers know. The practice is considering opening up their wireless Internet to patients (for use in the waiting room) using a separate, restricted guest account setup with the practice's router, but have not yet done so.

Eric checks his personal e-mail in the morning, using his Gmail account, secured by his use of the HTTPS Everywhere browser extension for the Google Chrome Web browser. He does not use his Gmail account to communicate with patients, instead using it primarily with friends and family and for shopping online. While replying to e-mail, he notices that his ClamXav antivirus software is running, checking for viruses. He also catches up on some patient notes using electronic records software that the clinic uses. The software backs up the data to a remote server, and the transmission is safe because he is using a secure wireless network, and the software company uses encrypted data transfers.

After seeing 3 consecutive patients, Eric visits a local coffee shop near his office to have lunch around 12:30 PM. *Using his password-protected iPad, he connects to their public Wi-Fi network and secures his connection by using the Cloak VPN.*

He connects to a US server to tunnel through (which is his default in the Cloak app user settings). Because his iPad is password-protected, he leaves it at his table while briefly using the restroom. He figures that there is a small possibility that it could be stolen while he is in the restroom, but he feels assured of the integrity of his data on the iPad because it is password-protected, and because he is using iOS 8, it is also encrypted. (Incidentally, iOS devices such as the iPad have remote locating software built in that also allows a remote wipe of the device if stolen.)

During his lunch, he surfs the Internet, reads the news online, and responds to personal e-mails. He receives an e-mail from one of his patients at his Riseup e-mail address, requesting a new appointment after a hiatus from treatment. He politely replies and asks the patient to contact the practice's secretary who maintains his schedule. He also receives an instant message on his phone's Wickr app from one of his patients with whom he allows instant messaging. The message is brief, from a patient informing Eric of her continued improvement, in response to Eric's prior suggestion to follow up with him between sessions. Accordingly, he replies to the message; by his default, his response is set to self-destruct in 2 days.

Subsequently, Eric uses his iPad to browse his personal Facebook feed and post a couple of photos of his family; his Facebook account is restricted to viewing by family and friends only, and he does not allow friend requests from patients. He also posts a couple of relevant mental health articles to his practice's Twitter account, which is open to the public. Of the practice's roughly 200 Twitter followers, some are patients (using pseudonyms) who prefer to receive tweets about general practice announcements; others follow the practice for the posted news articles that are relevant to mental health care.

After his lunch, Eric returns to his practice at 1:30 PM and sees several more patients. He leaves for the day at 5:30 PM and drives home to spend time with his family. Once home, he receives a call on his cell phone from his practice's answering service, notifying him that a patient called with a clinical emergency. He uses the Burner app on his phone to return the patient's call from a Burner number and handles the emergency on the phone. Eric has an uneventful evening at home with his family.

CONCLUSION

Privacy and security are important aspects of mental health care. Common practices for use of information technology in the digital age are not adequate for secure, HIPAA-compliant communication and record keeping. We recommend considering the implementation of the technology solutions we have discussed in this article.

Author affiliations: Department of Psychology, and Department of Psychiatry, University of Toledo, Toledo, Ohio (Dr Elhai); and Department of Psychology, University of Hawaii, Hilo; and the Menninger Clinic, Houston, Texas (Dr Frueh).

Potential conflicts of interest: The authors have no conflicts of interest to report. They have no association, financial or otherwise, with the software and apps mentioned in this article.

Funding/support: None reported.

REFERENCES

1. Aguilera A, Muench F. There's an app for that: information technology applications for cognitive behavioral practitioners. *Behav Ther (N Y N Y)*. 2012;35(4):65–73.
2. Sims H, Sanghara H, Hayes D, et al. Text message reminders of appointments: a pilot intervention at four community mental health clinics in London. *Psychiatr Serv*. 2012;63(2):161–168.
3. Kazdin AE, Blase SL. Rebooting psychotherapy research and practice to reduce the burden of mental illness. *Perspect Psychol Sci*. 2011;6(1):21–37.
4. Torous J, Friedman R, Keshavan M. Smartphone ownership and interest in mobile applications to monitor symptoms of mental health conditions. *JMIR Mhealth Uhealth*. 2014;2(1):e2.
5. Mojtabai R. Americans' attitudes toward mental health treatment seeking: 1990–2003. *Psychiatr Serv*. 2007;58(5):642–651.
6. Henderson C, Evans-Lacko S, Thornicroft G. Mental illness stigma, help seeking, and public health programs. *Am J Public Health*. 2013;103(5):777–780.
7. Bennett K, Bennett AJ, Griffiths KM. Security considerations for e-mental health interventions. *J Med Internet Res*. 2010;12(5):e61.
8. Taube DO. Portable digital devices: meeting challenges to psychotherapeutic privacy. *Ethics Behav*. 2013;23(2):81–97.
9. O'Harrow R. Health-care sector vulnerable to hackers, researchers say. *Washington Post*. December 25, 2012. http://www.washingtonpost.com/investigations/health-care-sector-vulnerable-to-hackers-researchers-say/2012/12/25/72933598-3e50-11e2-ae43-cf491b837f7b_story.html. Accessed April 21, 2015.
10. HIMSS. HIMSS Analytics 2013 Mobile Technology Survey examines mHealth landscape. http://himssanalytics.org/about/NewsDetail.aspx?nid=82148. Accessed February 26, 2014.
11. Van Allen J, Roberts MC. Critical incidents in the marriage of psychology and technology: a discussion of potential ethical issues in practice, education, and policy. *Prof Psychol*. 2011;42(6):433–439.
12. Koh S, Cattell GM, Cochran DM, et al. Psychiatrists' use of electronic communication and social media and a proposed framework for future guidelines. *J Psychiatr Pract*. 2013;19(3):254–263.
13. Medani A, Gani A, Zakaria O, et al. Review of mobile short message service security issues and techniques towards the solution. *Scientific Research and Essays*. 2011;6:1147–1165.
14. How it takes just 15 minutes of web tuition for anyone to hack into your email. *Daily Mail*. May 27, 2011. http://www.dailymail.co.uk/sciencetech/article-1391297/How-takes-just-15-minutes-web-tuition-hack-email.html. Accessed April 21, 2015.
15. Pagliery J. Half of American adults hacked this year. CNN Money website. http://money.cnn.com/2014/05/28/technology/security/hack-data-breach/. Updated March 28, 2014. Accessed April 21, 2015.
16. Greenwald G. *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State*. New York, NY: Metropolitan Books; 2014.
17. Greenwald G, MacAskill E, Poitras L. Edward Snowden: the whistleblower behind the NSA surveillance revelations. *The Guardian*. June 9, 2013. http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance. Accessed April 22, 2015.
18. Gordon W. How to turn your computer's firewall on and off for beginners. Lifehacker website. http://lifehacker.com/5805326/how-to-turn-your-computers-firewall-on-and-off. Updated May 25, 2011. Accessed April 22, 2015.
19. Purdy K. What settings should I change on my Wi-Fi router? Lifehacker website. http://lifehacker.com/5553789/what-settings-should-i-change-on-my-wi-fi-router. Updated June 10, 2010. Accessed April 21, 2015.
20. Abdul B. WiFi is getting even more public—don't make yourself a target. Forbes website. http://www.forbes.com/sites/groupthink/2014/07/14/wifi-is-getting-even-more-public-dont-make-yourself-a-target/. Updated July 14, 2014, Accessed April 22, 2015.
21. Henry A. Five best VPN service providers. Lifehacker website. http://lifehacker.com/5935863/five-best-vpn-service-providers. Updated March 23, 2014. Accessed April 22, 2015.
22. Richardson LK, Frueh BC, Grubaugh AL, et al. Current directions in videoconferencing tele-mental health research. *Clin Psychol (New York)*. 2009;16(3):323–338.
23. Frueh BC, Monnier J, Elhai JD, et al. Telepsychiatry treatment outcome research methodology: efficacy versus effectiveness. *Telemed J E Health*. 2004;10(4):455–458.
24. Asay M. Google Hangouts may be ready to eat videoconferencing. ReadWrite website. http://readwrite.com/2014/04/24/google-hangouts-skype-videoconferencing. Updated April 24, 2014. Accessed April 22, 2015.
25. Fleishman G. Skype and online privacy: called out. *The Economist*. July 30, 2012. http://www.economist.com/blogs/babbage/2012/07/skype-

and-online-privacy. Accessed April 22, 2015.

26. Henry A. How to encrypt your email and keep your conversations private. Lifehacker website. http://lifehacker.com/how-to-encrypt-your-email-and-keep-your-conversations-p-1133495744. Updated August 14, 2013. Accessed July 21, 2014.
27. Greenwald G. Email service used by Snowden shuts itself down, warns against using US-based companies. *The Guardian*. August 19, 2013. http://www.theguardian.com/commentisfree/2013/aug/09/lavabit-shutdown-snowden-silicon-valley. Accessed April 22, 2015.
28. DeJong SM, Gorrindo T. To text or not to text: applying clinical and professionalism principles to decisions about text messaging with patients. *J Am Acad Child Adolesc Psychiatry*. 2014;53(7):713–715.
29. Timberg C. Newest Androids will join iPhones in offering default encryption, blocking police. *Washington Post*. September 18, 2014. http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/. Accessed April 22, 2015.
30. Reader R. Tired of being spied on? these startups try to keep your secrets safe. VentureBeat website. http://venturebeat.com/2014/07/20/tired-of-being-spied-on-these-startups-try-to-keep-your-secrets-safe/. Updated July 20, 2014. Accessed April 22, 2015.
31. Cepelewicz BB. Text messaging with patients: steps physicians must take to avoid liability. Medical Economics website. http://medicaleconomics.modernmedicine.com/medical-economics/news/text-messaging-patients-steps-physicians-must-take-avoid-liability. Updated May 23, 2014. Accessed April 21, 2015.
32. Morris P. Best free encrypted messaging apps for iPhone. Redmond Pie website. http://www.redmondpie.com/best-free-encrypted-messaging-apps-for-iphone-list/. Updated March 9, 2014. Accessed April 21, 2015.
33. Electronic Frontier Foundation. Secure messaging scorecard: which apps and tools actual keep your messages safe? https://www.eff.org/secure-messaging-scorecard. Accessed April 21, 2015.
34. Henry A. The difference between antivirus and anti-malware (and which to use). Lifehacker website. http://lifehacker.com/the-difference-between-antivirus-and-anti-malware-and-1176942277. Updated August 21, 2013. Accessed April 21, 2015.
35. Gordon W. A beginner's guide to encryption: what it is and how to set it up. Lifehacker website. http://lifehacker.com/a-beginners-guide-to-encryption-what-it-is-and-how-to-1508196946. Updated January 27, 2014. Accessed April 21, 2015.
36. LeFebvre R. Make your Mac even more secure with a firmware password (OS X tips). Cult of Mac website. http://www.cultofmac.com/262215/make-mac-even-secure-firmware-password-os-x-tips/. Updated January 14, 2014. Accessed April 21, 2015.
37. Hoffman C. How to secure your computer with a BIOS or UEFI password. How-To Geek website. http://www.howtogeek.com/186235/how-to-secure-your-computer-with-a-bios-or-uefi-password/. Accessed April 3, 2014.
38. Electronic Frontier Foundation. Secure deletion. https://ssd.eff.org/en/module/how-delete-your-data-securely. Updated April 21, 2014. Accessed April 21, 2015.
39. Aguilar M. Cloud storage showdown: Google Drive, Dropbox, iCloud, and more compared. Gizmodo website. http://gizmodo.com/dropbox-google-drive-and-more-whats-the-best-cloud-st-1627423823. Updated August 27, 2014. Accessed April 21, 2015.
40. Gordon W. The always up-to-date guide to managing your Facebook privacy. Lifehacker website. http://lifehacker.com/5813990/the-always-up-to-date-guide-to-managing-your-facebook-privacy. Updated January 3, 2013. Accessed April 21, 2015.
41. Gordon W. Here's everywhere you should enable two-factor authentication right now. Lifehacker website. http://lifehacker.com/5938565/heres-everywhere-you-should-enable-two-factor-authentication-right-now. Updated December 10, 2013. Accessed December 10, 2013.