Curr Psychiatry Rep (2016) 18: 91
DOI 10.1007/s11920-016-0726-x

PSYCHIATRY IN THE DIGITAL AGE (JS LUO, SECTION EDITOR)

Mobile Mental Health: Navigating New Rules and Regulations for Digital Tools

James Armontrout[1] · **John Torous**[2,3] · **Matthew Fisher**[4] · **Eric Drogin**[2] · **Thomas Gutheil**[2,3]

Published online: 23 August 2016

Abstract Mobile health (mHealth) apps are becoming much more widely available. As more patients learn about and download apps, clinicians are sure to face more questions about the role these apps can play in treatment. Clinicians thus need to familiarize themselves with the clinical and legal risks that apps may introduce. Regulatory rules and organizations that oversee the safety and efficacy of mHealth apps are currently fragmentary in nature and clinicians should pay special attention to categories of apps which are currently exempt from significant regulation. Uniform HIPAA protection does not apply to personal health data that are shared with apps in many contexts which creates a number of clinically relevant privacy and security concerns. Clinicians should also consider several relatively novel potential adverse clinical outcomes and liability concerns that may be relevant to specific categories of apps, including apps that target (i) medication adherence, (ii) collection of self-reported data, (iii) collection of passive data, and (iv) generation of treatment recommendations for psychotherapeutic and behavioral interventions. Considering these potential pitfalls (and disclosing them to patients as a part of obtaining informed consent) is necessary as clinicians consider incorporating apps into treatment.

This article is part of the Topical Collection on *Psychiatry in the Digital Age*

✉ James Armontrout
james.armontrout@ucsf.edu

[1] University of California, San Francisco, 401 Parnassus Avenue Box PLP-0984, San Francisco, CA 94143-0984, USA

[2] Beth Israel Deaconess Medical Center, 330 Brookline Ave E/Rabb 2, Boston, MA 02115, USA

[3] Massachusetts Mental Health Center, Boston, USA

[4] Mirick O'Connell Attorneys at Law, Boston, USA

Keywords mHealth · Legal · Informed consent · Smartphone

Introduction

The outpatient appointment is about to end when the patient says there is "one more thing" she would like to discuss with her psychiatrist. She reaches into her pocket, pulls out a smartphone, and proceeds to ask if her psychiatrist recommends an app that the patient has heard about which tracks mood and offers "on-the-go mindfulness exercises." The psychiatrist realizes the potential for smartphone apps to offer novel adjunctive monitoring and support services for some patients but also wonders what may be the legal ramifications of using or recommending apps in clinical care.

Patients now have direct access to a rapidly increasing number of smartphone apps designed for healthcare—approximately 165,000 is the latest number [1]. While these apps are designed and marketed for virtually all healthcare conditions, apps related to mental health actually compose the largest single category [1]. Given the reality that today's psychiatric patients are increasingly web-connected [2], interested in apps [3, 4] and likely to own smartphones, it is certain that these persons will inquire about the role of smartphone apps more frequently.

Although the proliferation, allure, and ownership of mental health technologies like condition-specific smartphone apps and wearable sensors continue to increase, evidence for their clinical utility, efficacy, and safety is generally lacking [5, 6]. Additionally, there is an even greater lack of understanding (or literature-based guidance) regarding attendant legal issues. Clinicians need to understand not only the risks to patients but also the risks they themselves assume when utilizing or recommending digital technologies like smartphones as adjuncts to traditional psychiatric care. In this article, we review

some of the basic principles governing legal liability for smartphone app use and then provide a focused look at unique facets of various app technologies.

Understanding the Basic Rules and Regulations

Novel developments like smartphone apps and digital health technologies tend to spawn complex and rapidly evolving liability issues. Clinicians need to be aware of some basic legal principles and overarching federal rules while the finer points play out in regulatory rulemaking, lawsuits, legislative sessions, and the promulgation of updated professional standards. Here, we briefly introduce several important regulatory rules and organizations that govern much of the mobile health and mobile psychiatry landscape—in particular, the Health Insurance Portability and Accountability Act ("HIPAA"), the Food and Drug Administration ("FDA"), and the Federal Trade Commission ("FTC").

Clinicians may presume that any app related to healthcare falls under the ambit of HIPAA, a federal law mandating privacy and security standards for certain types of healthcare data. Yet, this is frequently not the case. HIPAA applies only to "covered entities" (which are healthcare providers, healthcare clearinghouses, or health plans), "business associates," or subcontractors of business associates. A business associate is defined as a third party that receives, maintains, or creates protected health information for or on behalf of any of a covered entity [7••]. HIPAA protections apply to protected health information, which is identifiable data that pertain to past, present, or future physical or mental health conditions, to the provision of healthcare, or to payment for such services [8].

The invocation of HIPAA is all about *context*. For example, it will initially be unclear whether HIPAA applies when a smartphone app that collects information on a patient's mood symptoms appears to be collecting personal health information as well. If a patient uses the app independently of a clinician's advice and does not transmit any of the data collected by the app, it is likely that the app falls completely outside of the HIPAA realm. By contrast, if a hospital contracts with this app's developers to provide it to the hospital's patients and then filter collected data to the hospital, then the developers are most likely acting as business associates of the hospital and its clinicians, which would in turn bring HIPAA protections to bear. The key to understanding whether HIPAA comes into play is understanding who is collecting the data, why the data are being collected, and who will use the data. Misassumptions about when HIPAA applies have led to significant privacy concerns [7••, 9] that we explore below in detail.

The FDA and the FTC both play roles in evaluating the safety and marketing claims of mobile health technologies, though neither agency is currently stepping in to provide full oversight of all apps. The Congress granted the FDA authority over medical devices—including medical software—with the 1976 Medical Device Amendment to the Federal Food, Drug, and Cosmetic Act. Since that time, medical software has been regulated by the FDA's Center for Devices and Radiological Health (CDRH) [10••]. The approval of new devices historically required stand-alone evidence of safety and effectiveness. An easier "me-too" conduit (the "510(k) Pathway") has frequently been used, whereby a new device seeking approval establishes "substantial equivalence" to an already approved device.

The 510(k) Pathway is in substantial danger of being swamped by the thousands of new smartphone apps now being released every month, or in some cases, may not apply to novel innovative apps. In response, the FDA has chosen to regulate apps based on the perceived level of concern they engender, calling for regulators to estimate "the severity of injury that a device could permit or inflict, either directly or indirectly, on a patient or operator as a result of device failures, design flaws, or simply by virtue of employing the device for its intended use" [11].

The FDA has also declined to regulate the large portion of arguably healthcare-related apps that fall into a "general wellness" category. Such apps "promote a healthy lifestyle" but do not make reference to any specific disease, diagnosis, or treatment [10••]. Examples given by the FDA include apps that provide information to users about gluten-free food, guide them about questions to ask their physician during visits, or help them to identify a pill based on its physical characteristics [12]. Although the FDA maintains the right to exercise "regulatory enforcement discretion" concerning such apps—and has already done so with some that relate to psychiatry [11]—the vast majority of apps are not FDA-regulated at this point in time.

The FTC has begun policing marketing claims asserted by various apps, and some have called for the FTC to provide comprehensive oversight for telehealth in particular [9]. Examples of apps that have faced FTC action for making claims lacking evidentiary support include (i) acne applications which purported to treat acne by shining a light from a smartphone on the user's face [13], (ii) an application which claimed to calculate a mole's risk of melanoma; [14], and (iii) a $2 million settlement against a "brain training" app (Lumosity) which purported to reduce or delay cognitive impairments associated with age or health conditions [15]. Given the sheer volume of apps flooding the marketplace and a reactive (rather than proactive) approach to the policing of claims, the FTC is currently serving a rather limited role in app regulation.

The private sector has also made limited forays into systematically certifying potential privacy and security vulnerabilities in medical apps. The startup Happtique reviewed the

operability, privacy, security, and content of apps and received some early attention but ultimately shut down after discovering that two apps it certified had handled data insecurely [16••]. The Consumer Electronics Association, which represents numerous technology member companies such as Apple, Google, Fitbit, and roughly 2000 others, recently announced the voluntary guidelines for companies should approach privacy for health-related data [17]. At this point, however, it is unclear if the private industry as a whole will adopt such guidelines, given that individual companies often have very different privacy policies and procedures for managing healthcare data and other related information.

Legal Concerns That Extend Across Application Types

Privacy and Security

A major concern in mobile health relates to patient privacy and security, concerning the potential for unintended breaches of data as well as the intentional transfer or sale of data to third parties [7••]. As discussed above, there are many contexts in which the protections created by HIPAA do not apply to healthcare apps. In these cases, the privacy policies that users accept when installing the app govern the use of the data generated or collected through the app. Relying on the privacy policies of the app developers themselves is fraught with danger; for example, a recent study noted that of the 600 most common apps, (1) only 31 % had privacy policies at all, (2) the required reading level of such policies was typically at a college level, and (3) 66 % of these privacy policies consisted of legal "boilerplate" that did not even mention the specific app in question [7••].

In the absence of HIPAA protections or strongly protective agreements around privacy, it is very possible that healthcare-related data may be collected and sold by the app company for uses that the patient never imagined. At present, data brokers may end up indefinitely owning the patient's data and using it for a variety of purposes—including generation of FICO Medication Scores, targeted advertisements, or larger profiling efforts [7••]. While some patients may accept the tradeoff of privacy for the convenience or other services offered by the app, others will not. Therefore, clinicians who recommend an app to a patient should understand and discuss not only the nature of the app but also who would own the data and how it could be used. Patients may already grasp that in many instances, HIPAA will not apply, but informed consent should be obtained and documented.

The potential for a breach of data by hackers or human error should also be considered. While we do not know of any specific lawsuits related to data compromised via mobile health apps, there *have* been lawsuits stemming from electronic data breaches more generally. For example, a class action lawsuit was recently filed after hackers potentially gained access to up to 4.5 million patient health records [18].

When a breach occurs, the covered entity (the clinician or healthcare facility) will likely face highly public and embarrassing scrutiny. All parties involved may be subject to a lawsuit, even if at first glance they may appear remotely liable at best. Determining the potential for actionable liability can be both time-consuming and expensive. Ultimately, there will always be some modicum of risk, as it is never completely possible to "contract away" the potential for legal action.

Validation and Potential Malfunction of Apps

In one recent survey, physicians cited a lack of evidence-based content as one primary concern in recommending apps for patients [19]. Recent reviews have also demonstrated a paucity of data on the overall popularity of mobile health apps [6, 20]. While some specific applications may have empirical backing, it is likely—given the number of mobile health apps available—that patients will present with apps untested for specific clinical efficacy or safety and perhaps wholly unknown to the clinician. If a clinician recommends an app that does not have firm empirical backing, and an adverse outcome occurs (for instance, when a clinician recommends an online app as treatment adjunctive to a pharmacological regimen, and the patient later attempts suicide), it may be argued successfully that the applicable standard of care was not met.

Unanticipated issues may well arise around the use of apps that have not undergone rigorous safety and efficacy testing. For instance, if an app provides inaccurate data that causes a clinician to mismanage a condition, how should liability be apportioned? Additionally, if a patient makes mistakes in the use of an app and this results in mismanagement of her condition, to whom will blame ultimately be assigned? [21] Clinicians should thus consider any available evidence for the efficacy of the app, in addition to the potential for damage in a particular case should the app malfunction. Clinicians should also consider whether they feel comfortable (and truly capable of) educating the patient in the use of the app in the same way that they would do so regarding the use of other medical devices or courses of treatment.

Failure to Act on Information

Another potential source of liability is failure to act upon information that, for any number of reasons, is never reviewed by the clinician. A patient might, for instance, enter information about escalating suicidal thoughts or potential adverse effects of medication in the mistaken belief that the clinician will review and act upon this information in between visits. If

app-generated data will *not* be automatically reviewed and acted upon, this must be clearly stated to the patient, along with a review of the practice's existing methods of communication for relaying urgent information. Additionally, clinicians who agree to review app-generated data at each visit and then forget to do so may be ultimately be held liable for failure to act appropriately on such information. If, however, the clinician has explicitly declined to conduct such a review (for instance, framing use of a medication adherence tracking app as nothing more than an easy way for the *patient* to track medication adherence), then the likelihood that the clinician would be held responsible may be reduced. Establishing an agreement around the use of any app with the patient may help to avoid misunderstandings that could lead to adverse outcomes.

Concerns Relevant to Specific Categories of Apps

Reviewing mHealth apps for psychiatry has enabled us to identify several different usage categories, including those that target (i) medication adherence, (ii) collection of self-reported data, (iii) collection of passive data, and (iv) generation of treatment recommendations for psychotherapeutic and behavioral interventions. Reference apps (such as Epocrates or the DSM 5 app) are also expanding but will not be explored in detail. The authors only note that, as with texts or online resources, clinicians should consider the reliability of the source of such reference materials before utilizing them in clinical practice. Below, we review potential liability concerns that are specific to each category.

Medication Adherence

One of the most common current uses of healthcare apps is medication tracking and adherence. Apps can help patients remember to take their medications and help them to record side effects as well as perceived efficacy. Such data may be able to help psychiatrists find the "right" antidepressant medication; pilot study results are promising [22].

Beyond the concerns cited above, a novel source of liability may arise if a medication-related app erroneously advises the patient to take medications other than as prescribed—or otherwise malfunctions—and the patient suffers harm. In such a case, it is unclear who is liable: the patient, the app makers, or the clinician. Whatever the ultimate apportionment of blame, it certainly appears prudent to consider and discuss, as a standard part of informed consent, any foreseeable harm from apps before recommending them in clinical practice.

"Active" and "Passive" Data Collection

A number of apps allow patients to complete self-report scales for monitoring purposes. Today's apps, however, are increasingly doing much more than surveying patients in real time. Clinicians need to understand what "passive" data are, how they can be collected, and the liability issues they may raise.

Passive data are those collected by means that do not require any user engagement or activity. For example, a smartphone may automatically collect location data via GPS sensors or social data via call and text logs. A fitness tracker could automatically collect step data as well as heart rate information or even data about the quality of a user's sleep [23]. In some ways, the gathering of passive data is an attractive option, since such activity amounts to a decreased burden on users, with results that are more objective in nature than self-report data. Early studies are already exploring how such passive GPS data is correlated with depression [24•], although at this point, the authoritative appraisals of clinical validity and utility of passive data are still nascent or outright lacking. This has not stopped commercial app development, however, and patients can easily access a host of apps or devices that promise to capture passive data.

If a clinician recommends such an app, privacy is one clear source of concern, above and beyond the already important privacy concerns associated with non-passive data apps. We should not presume that information collected by a passive data app or device will automatically be subject to HIPAA. The data would likely fall under HIPAA only after they are transmitted to a clinician and then only those data that are under the clinician's control. The data *could* be subject to HIPAA if the clinician and the app or device developer have arranged for passive data collection either for or on behalf of the clinician. Given that a reasonable patient would likely want to know the privacy implications of app use outside of the usual patient-clinician confidentiality structure, a clinician who recommends an app but fails to apprise patients of known privacy implications might plausibly be held liable based on failure to obtain proper informed consent. Such concerns are all the more relevant when one considers that passive data may reveal where a patient lives (via GPS data), track where a patient shops (via a store's Wi-Fi signals), and expose a patient's social network (via call and text logs).

Another legally relevant issue that arises with respect to passive data is the responsibility of the clinician when an app unexpectedly reveals evidence of inappropriate—and potentially actionable—behavior. For example, an app that uses GPS data to promote increased exercise by depressed patients could also detect evidence that the patient was present where and when a violent crime is alleged to have occurred. An app that uses voice data for mood monitoring may inadvertently record the patient's assault upon a young child. When a passive data app could reveal more than intended, clinicians must

anticipate and navigate all the more cautiously their professional and legal responsibilities—especially, of course, when such instances could involve mandated reporting.

Situations requiring a breach of confidentiality are relatively rare but are by no means outside the range of normal clinical practice. Learning of issues of child or elder abuse or neglect is likely to trigger mandated reporting [25, 26]. In a post-*Tarasoff* world learning of specific threats of harm to others may create a duty either to protect or to warn intended victims [27]. Additionally, learning that a patient poses a danger of self-harm may lead to involuntary civil commitment or to moving otherwise outside of the usual frame of the doctor-patient relationship.

Given established limits to confidentiality, clinicians should make reasonable efforts to anticipate whether information gleaned from the use of an app might require disclosure. The clinician should be transparent about what data are being collected and how these data are being used. Transparency may help avoid surprises that could serve as one of the "bad feelings" evident in the "bad feelings plus bad outcome" formula for litigation [28]. Importantly, clinicians should remember that any information they learn about through the data collected by an app must be held in confidence by the clinician unless it meets an established exception to confidentiality. In short, such information should be afforded the same protections as any collateral clinical information obtained by other means—and, as with other encounters, patients should be informed about the limits of confidentiality in the doctor-patient relationship.

Apps Which Recommend or Provide Treatment

Many psychiatric illnesses that can be treated with behavioral and psychological interventions may also potentially be addressed via smartphone interventions. There is increasing evidence that smartphone apps are feasible and potentially effective tools for delivering behavioral activation [29, 30] and cognitive behavioral therapy [31•, 32]. The potential for portable, personalized, and real-time therapies delivered via technology is appealing, although again, the evidence base is still nascent. Predictably, such limitations have not held back app developers with the result that today's patient can access many mobile therapies directly from digital devices.

One potential liability issue—especially when coaches are incorporated into the app's content delivery system—is the nature of the service rendered and whether appropriate licensing is in place. For instance, review of one online service which claims to offer cognitive behavioral therapy for social anxiety suggests that through their service, users can "overcome social anxiety" using "cognitive behavioral therapy (CBT), the gold standard for overcoming social anxiety." The "Terms of Service" page, however, clearly states that the site "does not provide medical advice" and is "for informational purposes only," and that "coaches are not licensed health care professionals and are not authorized to provide services requiring professional licensure such as psychotherapy." It is unclear whether such claims would stand up to scrutiny with regard to whether the service does indeed offer psychotherapy and whether assertions about services could be viewed as deceptive or misleading. Regardless, if a patient asks whether his or her clinician would recommend such a service as a psychotherapeutic experience, that clinician would need to discuss the service's perceived limitations and emphasize that by the site's own claims that it does not offer psychotherapy. We currently recommend abstaining from formal recommendation of such treatment apps unless and until evidence for efficacy of the app in question emerges.

Privacy law—including the potential applicability of HIPAA—is relevant to these circumstances. For the service mentioned above (which, if successful, other apps will likely try to replicate), it is stated that "if you submit or post any materials or content to this site, you grant us and our affiliates a royalty free, perpetual, irrevocable, transferrable, assignable, sub-licensable, worldwide license to use such materials and content, including alterations thereof, for our business purposes, in any form, in any media, and via any technology we choose, whether it exists now or is created in the future." While the specific ways in which posted information will ultimately be used is unclear, clinicians will again find it important to educate patients about the potential lack of confidentiality associated with apps offering "treatment" outside of a healthcare setting governed by HIPAA.

Conclusion

Mobile health apps have great potential to improve monitoring and treatment in the psychiatric context. At present, however, it must be acknowledged that these apps occupy a rather peculiar space in the world of psychiatric treatment. Empirical research about the real-world impact of apps on clinical care has not yet caught up with the plethora of apps available to consumers, and uniform standards for apps are not yet present. Also, as apps are not legally considered to be healthcare providers, issues of liability and confidentiality loom large, especially when patients may be unaware that the app with which they share their private health information is unlikely to hold this information confidential in the same way as would be expected of a clinician. Moreover, patients may be unaware that data collected by such apps are not protected by HIPAA and the app developers may not be subject to HIPAA-based penalties for any violation of confidentiality in many instances.

Ideally, in the future, information about the efficacy, reliability, and privacy of particular apps will be more easily

accessible and standardized. For now, we recommend that clinicians educate themselves to the extent practical about any given app before incorporating it into treatment, and that they hold informed consent discussions which disclose the known risks of app use in addition to the foreseeable "unknowns." Thinking of how we might discuss, educate, and prescribe a new medication is a useful model for thinking about how we might include apps in the clinical setting. While we know much about medications, our data on apps is still lacking—and the privacy concerns are greater. As mobile health continues to evolve, we nonetheless remain hopeful that over time, the unknowns will decrease and the benefits will become more compelling. Until then, clinicians need to be careful when using apps in clinical care and to ensure that they neither take on unexpected liability nor place patients in the way of unexpected harm.

Compliance with Ethical Standards

Conflict of Interest The authors declare that they have no conflict of interest.

Human and Animal Rights and Informed Consent This article does not contain any studies with human or animal subjects performed by any of the authors.

References

Papers of particular interest, published recently, have been highlighted as:
- • Of importance
- •• Of major importance

1. IMS. Patient Adoption of mHealth. 2015 2015-11-18; Available from: http://www.imshealth.com/en/thought-leadership/ims-institute/reports/patient-adoption-of-mhealth.
2. Firth, J., et al., Mobile phone ownership and endorsement of "mHealth" among people with psychosis: a meta-analysis of cross-sectional studies. Schizophr Bull, 2015
3. Torous J, Keshavan M, Gutheil T. Promise and perils of digital psychiatry. Asian J Psychiatr. 2014;10:120–2.
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. Firth J, Torous J. Smartphone apps for schizophrenia: a systematic review. JMIR Mhealth Uhealth. 2015;3(4):e102.
6. Torous J, Powell AC. Current research and trends in the use of smartphone applications for mood disorders. Internet Interv. 2015;2(2):169–73.
7. •• Glenn T, Monteith S. Privacy in the digital world: medical and health data outside of HIPAA protections. Curr Psychiatry Rep. 2014;16(11):494. **An important review of privacy implications related to mHealth**.
8. HHS. The Privacy Rule. 2013 2013-07-26 00:00:00.0; Available from: http://www.hhs.gov/.
9. Hall JL, McGraw D. For telehealth to succeed, privacy and security risks must be identified and addressed. Health Aff (Millwood). 2014;33(2):216–21.
10. •• Elenko E, Speier A, Zohar D. A regulatory framework emerges for digital medicine. Nat Biotechnol. 2015;33(7):697–702. **An important overview of the current regulatory environment**.
11. Center for Devices and Radiological Health, C.f.B.E.a.R. Search for FDA guidance documents—guidance for the content of premarket submissions for software contained in medical devices. [WebContent] 2015; Available from: http://www.fda.gov/RegulatoryInformation/Guidances/ucm089543.htm.
12. Health, C.f.D.a.R. Mobile medical applications—examples of MMAs that are not medical devices. [WebContent] 2015; Available from: http://www.fda.gov/MedicalDevices/DigitalHealth/MobileMedicalApplications/ucm388746.htm.
13. Dolan, B. US regulators remove two acne medical apps. 2011 2011-09-09 12/6/2015]; Available from: http://mobihealthnews.com/13123/us-regulators-remove-two-acne-medical-apps.
14. Katz, M. FTC cracks down on marketers of â€ œMelanoma Detectionâ€ Apps | Federal Trade Commission. 2015 12/6/2015]; Available from: https://www.ftc.gov/news-events/press-releases/2015/02/ftc-cracks-down-marketers-melanoma-detection-apps.
15. Lumosity to pay $2 million to settle FTC deceptive advertising charges for its â€ œBrain Trainingâ€ Program | Federal Trade Commission. 2016; Available from: https://www.ftc.gov/news-events/press-releases/2016/01/lumosity-pay-2-million-settle-ftc-deceptive-advertising-charges.
16. •• Powell AC, Landman AB, Bates DW. In search of a few good apps. JAMA. 2014;311(18):1851–2. **A viewpoint article which discusses the need for improved app review to improve app usefulness and bolster clinician and patient confidence**.
17. Dolan B. How health, fitness device makers should approach privacy, according to CEA. 2015. 2015-10-27; Available from: http://mobihealthnews.com/48010/how-health-fitness-device-makers-should-approach-privacy-according-to-cea.
18. Shivley N. UCLA sued over recent hospital records hacking. 2015. Available from: http://www.latimes.com/business/la-fi-ucla-hack-lawsuit-20150811-story.html.
19. Zhang Y, Koch S. Mobile health apps in Sweden: what do physicians recommend? Stud Health Technol Inform. 2015;210:793–7.
20. Donker T et al. Smartphones for smarter delivery of mental health programs: a systematic review. J Med Internet Res. 2013;15(11):e247.
21. Kluge EH. Ethical and legal challenges for health telematics in a global world: telehealth and the technological imperative. Int J Med Inform. 2011;80(2):e1–5.
22. Schaffer A et al. Use of mental health telemetry to enhance identification and predictive value of early changes during augmentation treatment of major depression. J Clin Psychopharmacol. 2013;33(6):775–81.
23. Duffy J. The best fitness trackers for 2015. 2015. Available from: http://www.pcmag.com/article2/0,2817,2404445,00.asp.
24. • Saeb S et al. Mobile phone sensor correlates of depressive symptom severity in daily-life behavior: an exploratory study. J Med Internet Res. 2015;17(7):175. **Original research study showing potential predictive value of passive data (as collected by sensors) in major depression**.
25. DHHS. State laws. 2015. Available from: http://www.ncea.aoa.gov/Library/Policy/Law/State/index.aspx.
26. MGL. General laws: CHAPTER 119, section 51A. 2015. Available from: https://malegislature.gov/Laws/GeneralLaws/PartI/TitleXVII/Chapter119/Section51A.
27. Felthous AR. Warning a potential victim of a person's dangerousness: clinician's duty or victim's right? J Am Acad Psychiatry Law. 2006;34(3):338–48.

28. Gutheil TG, Bursztajn H, Brodsky A. Malpractice prevention through the sharing of uncertainty. Informed consent and the therapeutic alliance. N Engl J Med. 1984;311(1):49–51.
29. Ly KH et al. Smartphone-supported versus full behavioural activation for depression: a randomised controlled trial. PLoS One. 2015;10(5):e0126559.
30. Ly KH et al. Behavioural activation versus mindfulness-based guided self-help treatment administered through a smartphone application: a randomised controlled trial. BMJ Open. 2014;4(1):e003440.
31.• Dagoo J et al. Cognitive behavior therapy versus interpersonal psychotherapy for social anxiety disorder delivered via smartphone and computer: a randomized controlled trial. J Anxiety Disord. 2014;28(4):410–7. **An original study showing a 55.6 % response rate to a mobile phone-administered CBT intervention in social anxiety disorder**.
32. Watts S et al. CBT for depression: a pilot RCT comparing mobile phone vs. computer. BMC Psychiatry. 2013;13:49.