AMA Journal of Ethics®
September 2018, Volume 20, Number 9: E864-872

POLICY FORUM

How Could Commercial Terms of Use and Privacy Policies Undermine Informed Consent in the Age of Mobile Health?

Cynthia E. Schairer, PhD, Caryn Kseniya Rubanovich, MS, and Cinnamon S. Bloss, PhD

Abstract

Granular personal data generated by mobile health (mHealth) technologies coupled with the complexity of mHealth systems creates risks to privacy that are difficult to foresee, understand, and communicate, especially for purposes of informed consent. Moreover, commercial terms of use, to which users are almost always required to agree, depart significantly from standards of informed consent. As data use scandals increasingly surface in the news, the field of mHealth must advocate for user-centered privacy and informed consent practices that motivate patients' and research participants' trust. We review the challenges and relevance of informed consent and discuss opportunities for creating new standards for user-centered informed consent processes in the age of mHealth.

Privacy and Informed Consent in the Age of Mobile Health

Mobile health (mHealth) refers to the use of technologies such as smartphone apps or wearable sensors to monitor health. In the past decade, there has been increasing enthusiasm for the role of mHealth in promoting precision medicine and learning health systems.[1] However, there are significant risks to collecting, transmitting, and storing personal health data that experts and the public alike have been slow to recognize. Current news about the sheer amount of data shared or sold by health technology companies and by platforms like Facebook, the lack of transparency about these activities, and the many possible malicious uses of these data have sparked a "techlash" reflecting public unease about many technologies central to mHealth research and clinical care.[2-4] In the current climate, demonstrating a clear and consistent commitment to the tenets of informed consent will be more important than ever for conscientious scientists and health care practitioners who wish to maintain the trust of participants and patients involved in mHealth studies or clinical interventions.

Informed Consent in mHealth

Whether used for precision medicine research, health-related citizen science, *N*-of-1 studies, or clinical care, mHealth tools pose challenges for the process of obtaining meaningful informed consent from users.[5-8] The sensitivity and value of health information, along with the complexity of mHealth ecosystems, create unique privacy risks that are difficult to foresee and understand.[7,9,10] The risks are wide ranging and can include insurance discrimination based on data from mHealth technologies integrated into workplace wellness programs,[11] inadvertent invasion of privacy of family members or other "bystanders" with collection of data in home environments,[12] compromising community safety (as in military presence recently revealed by the Strava app[13,14]), and political manipulation through profiling based on health data, which has the potential to be far more personal than Facebook posts.[2,15] In many mHealth contexts, use of remote consent can exacerbate communication difficulties, especially if traditional informed consent forms are simply migrated to remote platforms. Improvements to the informed consent process, such as Sage Bionetworks eConsent for the Apple ResearchKit Parkinson mPower study,[16,17] rely on researcher initiative and commitment to implement such innovations.[18,19]

Among the many challenges to informed consent in mHealth, the problem of reconciling commercial terms of use with informed consent is perhaps most pressing for the field. Compared to most commercial contexts, the Common Rule[20] and the Health Insurance Portability and Accountability Act (HIPAA) set high standards for the protection of patient and research participant data in medical settings. However, cost effective applications of mHealth technologies in medical care and research depend on bringing apps and devices developed in commercial contexts into medical settings. Maintaining a high standard of privacy protection in research and health care utilizing mHealth technologies will require attention to important differences between informed consent and commercial terms of use documents—specifically, differences in readability, content, and the protections afforded. We argue that the principles that underlie informed consent should guide professionals who adopt mHealth technology as they seek to maintain transparency and protect the interests of mHealth participants and patients. If legitimate health research and care are to incorporate these tools, health professionals and their institutions must work to promote transparency and public trust by addressing the challenges to informed consent. We point to opportunities for institution-based researchers to lead the way in this effort.

Ubiquity of Commercial Terms of Use and Privacy Policies

The unique obstacle for mHealth with respect to informed consent is that users—whether research participants, patients, or "lifeloggers" (people who digitally record all aspects of their lives)—are nearly always required to agree to terms of use of the underregulated commercial entities supplying mHealth devices and services. Typical terms of use for commercially developed apps and devices, including those used in

research, include lengthy legalese and may stipulate the release or selling of personal identifiable data,[9,10,21-24] thus representing a significant departure from the principles of informed consent. Moreover, in medical settings, institutional review boards (IRBs) often require clear and explicit language stating risks—including risks to privacy—as well as statements of how confidentiality will be protected, but there is a challenge in reconciling IRB-approved informed consent documents with the terms of use set forth by commercial entities.[25]

While some researchers might have the resources and expertise to develop their own devices or apps, in most cases mHealth researchers will make use of commercially available tools for their studies. In these cases, researchers broker a relationship between study participants and the company supplying the technologies or acting as the first point of collection for the data. Thus, they are put in the position of requiring that participants accept commercial terms of use as a condition of study participation, thereby subjecting participants to any risks related to those terms. Furthermore, the number of required documents proliferates for each sensor, smartphone, app, or data service used. For example, a study led by the senior author (CSB) required participants to agree to up to 5 different terms of use documents in addition to an IRB-approved informed consent.[26] Requiring participants to review such a large number of agreements makes it less likely that they will be able to devote the necessary energy to understand the content before consenting, rendering such consent "uninformed" rather than informed. In theory, this situation could be an opportunity for researchers to protect participants from questionable consumer contracts or commercial use of their data, either by subjecting commercial terms of use to IRB review or by negotiating with companies to create more user-centered terms of use. In practice, however, IRBs may or may not have adequate resources or expertise to thoroughly evaluate these terms. In addition, companies may resist changes to these terms as they are designed to limit their legal exposure and protect their commercial interests. The burden of convincing companies to incur the potential liability and expense of altering terms of use cannot be borne by individual researchers or clinicians,[27] and hence this task requires collective action.

Continued Importance of Informed Consent in the Age of mHealth

The tradition of informed consent will serve as an invaluable resource for the field of mHealth as it faces the challenge of protecting user interests in privacy and transparency. Maintaining public trust and willingness to engage with new technologies is, after all, essential to realizing the power of mHealth to improve both individual and population health.

Studies of attitudes toward data sharing indicate that people prefer to be asked for permission to use their data in research, especially when health information is involved.[6,28-31] A recent survey showed that 68% of users of digital self-tracking

technologies said they would share personal health information "if privacy were assured" and 67% felt anonymity was "very" or "extremely" important.[6] Another survey found that respondents across generations were concerned about health privacy,[32] contrary to popular assumptions about millennial disinterest in privacy. While it might be assumed that early adoption of health technologies is coupled with a disinterest in privacy, a qualitative study of privacy attitudes among early adopters of personal wearable sensors and health apps demonstrated that members of this group placed a value on personal data privacy and expressed the desire to control their personal data.[31] Such findings underscore the importance of notification about data uses and consent in maintaining relations of trust when asking for personal health information.

The European Union's (EU's) new General Data Protection Regulation (GDPR) is another indication of current interest in protecting privacy and in transparent consent. The GDPR requires that, in most commercial situations, contracts present explicit opportunities for signers to consent to the collection and use of any personal information.[33] Furthermore, the GDPR demands that requests for consent be legible and accessible, that the purpose of collecting data be stated, and that consent be obtained at the point of data collection and be easy to withdraw.[34,35] While not law outside of the EU, the GDPR reflects some common expectations about privacy and has the potential to become an international gold standard for individuals concerned about their personal privacy.

Opportunities to Promote Informed Consent and the Protection of Privacy

In our view, the challenges we have raised are best approached as opportunities for health care and research institutions seeking to leverage mHealth technologies to lead the important work of creating user-centered informed consent procedures.

The first step for those who wish to incorporate mHealth into medical research or clinical practice is to be aware that commercial data collection, transmission, storage, access, and use are underregulated and not standardized. For this reason, researchers and physicians should take the opportunity to be savvy consumer advocates when selecting the products they recommend and keep in mind that commercial partners typically use collected data for their own purposes. As an example, Fitabase, a company that serves as a bridge between academic researchers and Fitbit, a company that makes devices and apps to monitor fitness-related metrics, suggests that researcher-initiated strategies for protecting privacy such as creating anonymous Fitbit accounts with limited demographic data, not collecting GPS data, and maintaining a schedule for deleting data could be worthwhile.[36]

Ultimately, though, what is needed are strategies to ensure that data-sharing practices are safe and transparent without limiting the potential of mHealth tools to improve health. The GDPR is one attempt to reign in current unregulated activities through a comprehensive law, but the strategies the GDPR uses are similar to, and perhaps more

stringent than, HIPAA and the Common Rule, which some argue strangle 21st century US medical research.[37] In an attempt to facilitate research, recent changes to the Common Rule have expanded exemptions for informed consent,[6,7] but expanding exemptions may become an increasingly unpopular option for mHealth research as the public becomes more concerned about privacy in relation to consumer devices and apps. Other ideas include individualized or granular consent[38] or adopting "opt out" policies in certain contexts such as learning health care systems where the potential benefits of mHealth research for collective health may outweigh the importance of individual autonomy. Finally, Evans[39] has suggested a model of health data commons—new systems of governance that would allow individuals to lend their health data to research as part of a collective that would democratically set the terms for data use. All these approaches are ways to reinvent informed consent. Even the innovation of a data commons would not be the lack of consent—individuals would make the choice to join or leave the collective—but rather the opportunity to collectively negotiate the terms of that consent.

The national Precision Medicine Initiative project, All of Us, may be well situated to lead in creating user-centered terms of use for mHealth users. All of Us aims to enroll "one million or more people living in the United States" in the largest precision medicine cohort study to date.[40] Participants will be asked to contribute information via mHealth platforms in addition to genetic material and survey responses. The wide reach, resources, and scale of All of Us affords a unique opportunity for the cooperating institutions to negotiate with commercial partners for terms of use that meet stricter standards for both the presentation of informed consent documents and the data handling practices they use. This goal might be accomplished, for example, by creating a consortium of mHealth researchers working under the umbrella of All of Us to purchase products and services together under conscientious privacy policies designed to minimize data sharing among commercial partners. At present, we are not aware of any such coordinated efforts. Whatever policies and practices are developed by All of Us could serve as a model for smaller precision medicine projects as well as set a standard for handling mHealth data in any context.

Conclusion

Leaders in health care and research who seek to leverage mHealth technologies should draw upon the strength of informed consent as they face the challenge of managing unique privacy risks to users. For research participants and patients, informed consent expresses an exercise of autonomy and choice and is a symbol of professionals' good faith to handle personal data with integrity and transparency. Informed consent can strengthen trust in relationships across research and clinical practice, and therefore research and health care institutions should seek opportunities to promote and develop better systems of consent and oversight in the age of mHealth.

References

1. Steinhubl SR, Muse ED, Topol EJ. Can mobile health technologies transform health care? *JAMA*. 2013;310(22):2395-2396.
2. Lee MYH, Timberg C. How Cambridge Analytica broke into the US political market through Mercer-allied conservative groups. *Washington Post*. March 23, 2018. https://www.washingtonpost.com/politics/how-cambridge-analytica-broke-into-the-us-political-market-through-mercer-allied-conservative-groups/2018/03/23/141adba8-2ead-11e8-b0b0-f706877db618_story.html?utm_term=.8c858252e3fc. Accessed April 6, 2018.
3. King J. Facebook fallout: American's privacy at risk across entire tech, information industry. University of California. https://www.universityofcalifornia.edu/news/facebook-fallout-americans-privacy-risk-across-entire-tech-information-industry?utm_source=fiat-lux&utm_medium=internal-email&utm_campaign=article-general&utm_content=text. Published March 22, 2018. Accessed March 25, 2018.
4. Shah H. Use our personal data for the common good. *Nature*. 2018;556(7699):7.
5. Samuel JP, Burgart A, Wootton SH, Magnus D, Lantos JD, Tyson JE. Randomized *n*-of-1 trials: quality improvement, research, or both? *Pediatrics*. 2016;138(2):e20161103. doi:10.1542/peds.2016-1103.
6. Bietz MJ, Bloss CS, Calvert S, et al. Opportunities and challenges in the use of personal health data for health research. *J Am Med Inform Assoc*. 2016;23(e1):e42-e48. doi:10.1093/jamia/ocv118.
7. Rothstein MA, Wilbanks JT, Brothers KB. Citizen science on your smartphone: an ELSI research agenda. *J Law Med Ethics*. 2015;43(4):897-903.
8. Grady C, Cummings SR, Rowbotham MC, McConnell MV, Ashley EA, Kang G. Informed Consent. *N Engl J Med*. 2017;376(9):856-867.
9. Roosa S. A deep dive into the privacy and security risks for health, wellness and medical apps. IAPP. https://iapp.org/news/a/a-deep-dive-into-the-privacy-and-security-risks-for-health-wellness-and-medical-apps/. Published April 6, 2015. Accessed March 20, 2018.
10. Privacy Rights Clearinghouse. Mobile health and fitness apps: what are the privacy risks? https://www.privacyrights.org/consumer-guides/mobile-health-and-fitness-apps-what-are-privacy-risks. Published July 1, 2013. Updated December 16, 2016. Accessed March 26, 2018.
11. Wicklund E. mHealth-based workplace wellness programs face congressional scrutiny. mHealth Intelligence. https://mhealthintelligence.com/news/mhealth-based-workplace-wellness-programs-face-congressional-scrutiny. Published March 13, 2017. Accessed March 28, 2018.
12. Nebeker C, Lagare T, Takemoto M, et al. Engaging research participants to inform the ethical conduct of mobile imaging, pervasive sensing, and location tracking research. *Transl Behav Med*. 2016;6(4):577-586.

13. Nurse JRC. Strava storm: why everyone should check their smart gear security settings before going for a jog. Conversation. http://theconversation.com/strava-storm-why-everyone-should-check-their-smart-gear-security-settings-before-going-for-a-jog-90880. Published January 31, 2018. Accessed March 28, 2018.
14. Hsu J. The Strava heat map and the end of secrets. *Wired*. January 29, 2018. https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/. Accessed Feb 9, 2018.
15. Frenkel S, Benner K. To stir discord in 2016, Russians turned most often to Facebook. *New York Times*. February 17, 2018. https://www.nytimes.com/2018/02/17/technology/indictment-russian-tech-facebook.html. Accessed April 6, 2018.
16. Doerr M, Suver C, Wilbanks J. Developing a transparent, participant-navigated electronic informed consent for mobile-mediated research. Social Science Research Network. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769129. Published April 22, 2016. Accessed March 20, 2018.
17. Doerr M, Maguire Truong A, Bot BM, Wilbanks J, Suver C, Mangravite LM. Formative evaluation of participant experience with mobile eConsent in the app-mediated Parkinson mPower study: a mixed methods study. *JMIR Mhealth Uhealth*. 2017;5(2):e14. doi:10.2196/mhealth.6521.
18. ResearchKit. Obtaining consent. http://researchkit.org/docs/docs/InformedConsent/InformedConsent.html. Updated September 26, 2017. Accessed March 22, 2018.
19. Ouellette J. Apple's health experiment is riddled with privacy problems. *Gizmodo*. July 21, 2016. https://gizmodo.com/apple-s-health-experiment-is-riddled-with-privacy-probl-1783878924. Accessed March 24, 2018.
20. Federal policy for the protection of human subjects; final rule. *Fed Regist*. 2017;82(12):7149-7274. https://www.gpo.gov/fdsys/pkg/FR-2017-01-19/pdf/2017-01058.pdf. Accessed July 26, 2018.
21. Das G, Cheung C, Nebeker C, Bietz M, Bloss C. Privacy policies for apps targeted toward youth: descriptive analysis of readability. *JMIR Mhealth Uhealth*. 2018;6(1):e3. doi:10.2196/mhealth.7626.
22. Sunyaev A, Dehling T, Taylor PL, Mandl KD. Availability and quality of mobile health app privacy policies. *J Am Med Inform Assoc*. 2015;22(e1):e28-e33. doi:10.1136/amiajnl-2013-002605.
23. Steinhubl SR, Muse ED, Topol EJ. The emerging field of mobile health. *Sci Transl Med*. 2015;7(283):283rv3. doi:10.1126/scitranslmed.aaa3487.
24. Peppet SR. Regulating the internet of things: first steps toward managing discrimination, privacy, security and consent. *Tex Law Rev*. 2014;93:85-178.

25. Nebeker C, Harlow J, Espinoza Giacinto R, Orozco-Linares R, Bloss CS, Weibel N. Ethical and regulatory challenges of research using pervasive sensing and other emerging technologies: IRB perspectives. *AJOB*. 2017;8(4):266-276.
26. Bloss CS, Wineinger NE, Peters M, et al. A prospective randomized trial examining health care utilization in individuals using multiple smartphone-enabled biosensors. *PeerJ*. 2016;4:e1554. doi:10.7717/peerj.1554.
27. Bloss C, Nebeker C, Bietz M, et al. Reimagining human research protections for 21st century science. *J Med Internet Res*. 2016;18(12):e329. doi:10.2196/jmir.6634.
28. Tomlinson T, De Vries R, Ryan K, Kim H, Lehpamer N, Kim S. Moral concerns and the willingness to donate to a research biobank. *JAMA*. 2015;313(4):417-419.
29. Botkin JR, Rothwell E, Anderson R, Stark LA, Mitchell J. Public attitudes regarding the use of electronic health information and residual clinical tissues for research. *J Community Genet*. 2014;5(3):205-213.
30. Riordan F, Papoutsi C, Reed JE, Marston C, Bell D, Majeed A. Patient and public attitudes towards informed consent models and levels of awareness of electronic health records in the UK. *Int J Med Inform*. 2015;84(4):237-247.
31. Cheung C, Bietz MJ, Patrick K, Bloss CS. Privacy attitudes among early adopters of emerging health technologies. *PLoS One*. 2016;11(11):e0166389. doi:10.1371/journal.pone.0166389.
32. Pereira S, Robinson JO, Peoples HA, et al. Do privacy and security regulations need a status update? Perspectives from an intergenerational survey. *PLoS One*. 2017;12(9):e0184525. doi:10.1371/journal.pone.0184525.
33. Council of the European Union, European Parliament. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
34. Luger E, Moran S, Rodden T. Consent for all: revealing the hidden complexity of terms and conditions. In: Proceedings of the SIGCHI conference on Human factors in Computing Systems; April 27-May 2, 2013; Paris, France:2687-2696.
35. EU General Data Protection Regulation. GDPR key changes: an overview of the main changes under GDPR and how they differ from the previous directive. https://www.eugdpr.org/key-changes.html. Accessed February 23, 2018.
36. Fitabase. Fitabase security and privacy information. https://www.fitabase.com/media/1718/fitabase-security-and-privacy.pdf. Accessed March 19, 2018.
37. Evans BJ. Barbarians at the gate: consumer-driven health data commons and the transformation of citizen science. *Am J Law Med*. 2016;42(4):651-685.
38. Kim H, Bell E, Kim J, et al. iCONCUR: informed consent for clinical data and bio-sample use for research. *J Am Med Inform Assoc*. 2017;24(2):380-387.

39. National Institutes of Health. All of Us research program website. https://allofus.nih.gov/. Accessed February 23, 2018.

Cynthia E. Schairer, PhD is a postdoctoral fellow at the University of California, San Diego School of Medicine in La Jolla. She is a sociologist and qualitative researcher with an interest in the ethics of cutting edge technology in medicine and public health.

Caryn Kseniya Rubanovich, MS is a doctoral student in the San Diego State University-University of California, San Diego Joint Doctoral Program in Clinical Psychology. She is interested in the role of emerging technologies in clinical care and how these technologies impact clinician-patient relationships. She attained an AB in anthropology from Washington University and an MS in narrative medicine from Columbia University.

Cinnamon S. Bloss, PhD is an associate professor in the Department of Psychiatry and the Department of Family Medicine and Public Health in the Division of Health Policy at the University of California, San Diego in La Jolla. She also holds an adjunct appointment as a policy analyst at the J. Craig Venter Institute and is a licensed clinical psychologist. Her research focuses on the individual and societal impacts of emerging technologies in science, medicine, and public health.

Citation
AMA J Ethics. 2018;20(9):E864-872.

DOI
10.1001/amajethics.2018.864.

Acknowledgements
This work was supported by a grant from the National Institutes of Health National Human Genome Research Institute (R01 HG008753; C.S. Bloss, PI).

Conflict of Interest Disclosure
The author(s) had no conflicts of interest to disclose.

The viewpoints expressed in this article are those of the author(s) and do not necessarily reflect the views and policies of the AMA.

ISSN 2376-6980