CLINICAL TRIALS

Clinical Trials
2021, Vol. 18(5) 606–614

DOI: 10.1177/17407745211027245
journals.sagepub.com/home/ctj
SAGE

Navigating the ethics of remote research data collection

Luke Gelinas[1,2], Walker Morrell[2], Sarah A White[2] and Barbara E Bierer[2,3]

Abstract

COVID-19 has accelerated broad trends already in place toward remote research data collection and monitoring. This move implicates novel ethical and regulatory challenges which have not yet received due attention. Existing work is preliminary and does not seek to identify or grapple with the issues in a rigorous and sophisticated way. Here, we provide a framework for identifying and addressing challenges that we believe can help the research community realize the benefits of remote technologies while preserving ethical ideals and public trust. We organize issues into several distinct categories and provide points to consider in a table that can help facilitate ethical design and review of research studies using remote health instruments.

Keywords

Mobile health, research ethics, remote monitoring

Background

Remote data collection platforms, sometimes referred to as mobile health or "mHealth" technologies—telehealth, social media, mobile applications, smart devices, and wearables—are being increasingly leveraged in clinical research.[1] Such mHealth platforms have been used selectively in research for some time.[1] While the COVID-19 pandemic has accelerated their use, permitting remote data collection and allowing research to continue in ways that cohere with public health guidelines,[2–11] numerous independent factors also support the rise of mHealth technologies. Mobile technologies, ubiquitous in current society,[12,13] permit the capture and transmission of an increasingly wide array of physiological information (such as heart and respiratory rate, body temperature, blood sugar, and oxygen saturation) and the collection of patient reported outcome data in real time.[14] The technologies themselves are relatively inexpensive and their use avoids a number of costs associated with traditional research conduct, including time-consuming in-person interactions between participants and researchers. Importantly, mHealth also promises benefits for participants. Using mHealth data collection techniques in place of in-person study visits can promote participant autonomy by providing more control and flexibility over the research experience. The convenience of mHealth technologies has the potential to improve access to research, enabling participation for under-served individuals in low-resource settings, including people in lower- and middle-income countries.[15,16]

mHealth platforms are versatile research tools. They may be used as data management modalities, that is, as validated mechanisms for collecting, storing, and transmitting research data. They may also themselves be the object of research investigations, in two ways. First, mHealth studies may seek to establish the reliability of unvalidated mHealth interventions for a specific medical indication, such as when a wearable is evaluated for detecting atrial fibrillation. Second, mHealth studies may seek to evaluate the real-world health impact of using validated mHealth technologies themselves to change behavior, such as when a study evaluates whether medication adherence is impacted by notifying wearers of the onset of atrial fibrillation via a validated wearable. The greater the use and demand for validated mHealth data management tools, the greater the need

[1]Advarra IRB, Columbia, MD, USA
[2]Multi-Regional Clinical Trials Center of Brigham and Women's Hospital and Harvard, Cambridge, MA, USA
[3]Brigham & Women's Hospital, Harvard Medical School, Boston, MA, USA

Corresponding author:
Luke Gelinas, 6100 Merriweather Dr., Suite 600, Columbia, MD 21044, USA.
Email: luke.gelinas@advarra.com

for validation studies and insight into how mHealth impacts real-world health behaviors.

Research uses of mHealth technologies raise ethical issues that have yet to be fully articulated and addressed, leading to uncertainty and potentially hindering widespread adoption of their use.[17–21] In the United States, with its patchwork regulatory and oversight system, some research uses of mHealth technologies will be subject to US Food and Drug Administration and/or Health and Human Services ("Common Rule") regulations, while other uses may fall outside regulatory purview altogether (e.g. independent researchers and citizen science research).[22] Moreover, in public health emergencies, regulatory authorities have the power to waive or modify standard oversight processes and protections, including institutional review board (IRB) review.[23,24] While our main focus here is on regulated research that is subject to research ethics or IRB oversight, much of what we say can also contribute to a general framework for identifying and assessing the ethical issues with mHealth research and enabling sensible mitigation strategies.

We organize the ethical issues with research uses of mHealth into five areas: (1) data and reporting integrity, (2) privacy and confidentiality, (3) monitoring and the expectation of care, (4) implications of returning results via mHealth platforms, and (5) justice and access. We unpack the ethical challenges in the body of the article and provide actionable points-to-consider in Table 1. Given that mHealth technologies must be evaluated in their research-specific context, we take a primarily procedural approach and focus on identifying the issues that should be considered when evaluating these technologies, making more directive and concrete recommendations when possible.

Data and reporting integrity

mHealth platforms can be used for both active and passive data collection, which differ in terms of the intentional contribution made by the participant. Active data collection occurs when participants intentionally complete study activities, surveys, or other patient reported outcome measures using mHealth technology. Passive data collection occurs when devices operate in the background, recording information about participant's physiology or behavior (e.g. heart rate, oxygen saturation, steps), or using background audio or video recording to capture features of the user and their environment, without self-conscious interaction by users. Data collection may take place on a participant's own device that they bring to the research study, or with a device that is supplied to them as part of participation. Once collected, data are either stored on the device for later access, stored in the cloud, or transmitted via wireless networks to the research team or sponsor. Data that are stored in the cloud or transmitted via wireless networks may be monitored on an incoming basis or viewed periodically or once data collection is complete.

Active mHealth data collection is in some ways analogous to in-person completion of study activities, but also involves increased, and distinctive, data integrity risks. When interacting face-to-face with participants, researchers can be confident that participants are undertaking study procedures and tasks, investing time in answering surveys and questionnaires, and generally making a good-faith effort at completing study requirements. By contrast, it is not always possible to confirm these things for remote data collection. It may be challenging to confirm, for example, that it is the participant's steps being tracked with a wearable, rather than someone else who is wearing it, or that it is the participant rather than someone else who is completing required surveys and questionnaires. While researchers should not impugn the motives of participants, efforts to educate participants about data integrity, and provide support on the correct use of mHealth technologies, are wise. Researchers may take additional steps to ensure reliability as needed, such as observing and assisting participants with study activities via telehealth appointments, as a component of routine monitoring or when concerns about data integrity arise.

The large amounts of data generated by mHealth technologies are part of their promise, as continuous monitoring may enable the collection of real-world data points that would otherwise be missed, such as transient spikes in glucose or blood pressure. However, the collection of such large data sets also raises data integrity concerns.[25] These concerns stem both from the potential for error in the handling and transmission of large data sets, particularly when third-party vendors are involved, as well as the possibility for greater latitude in how they are analyzed. Large and complex data sets may enable statistical analyses that appear more favorable and supportive of study hypotheses than they truly are and that are more difficult to replicate in confirmatory studies. Because of this, data analysis plans for mHealth studies warrant increased attention from both researchers and ethical review bodies.

Sponsors and researchers should, when designing mHealth protocols, take special care to be precise about the plans for data and statistical analysis, specifying in detail which data points will be used for assessing which objectives and which data will be retained and used for assessing exploratory or future objectives. The plans for any excess data collected (i.e. data that will not be used to assess study objectives) should also be specified, with potential future or secondary uses clearly disclosed to participants. As a best practice, research stakeholders should consider adhering to the CONSORT-EHEALTH guidelines for reporting data collected by mHealth platforms.[26] Among other things, these guidelines require researchers to provide

Table 1. Points to consider in the design and review of mHealth research.

Category	Points to consider
Data and reporting integrity	• Does the potential exist for someone who is not the research participant to supply study data (e.g. for a mHealth device to be worn for study interventions by someone other than the participant)? ○ If yes, does the study team intend to educate participants about the importance of data integrity? ○ Are measures for ensuring reliability available as needed (such as video calls to observe required study behaviors)? ○ Are there additional measures to monitor data for reliability and completeness? • Does the protocol contain a clear data and statistical plan? ○ Is it clearly specified which data points will be used to assess which objectives? ○ Is incidental data collection minimized? ○ Are the plans for any incidental data that are collected clearly specified and their future use or destruction clear? • Are public registration obligations recognized in the protocol or consent documents? • Will the researchers adhere to the CONSORT-EHEALTH guidelines for reporting data from mHealth technologies?
Privacy and confidentiality	• Data collection ○ Is it possible to provide a device issued by the study team for the duration of the study? ■ If yes, have all functions of that device that may collect data extraneous to the research been disabled? ■ If no, will participants be asked to download mobile applications to their personal smart devices? • If yes, will the application have access to other sources of personal data on the participant's device? • Does the informed consent document clarify all the data that will be or can be accessed? ○ Is all of the data being collected necessary for research aims and objectives? ■ If data extraneous to the research is being collected, is there a compelling rationale? ○ Will geolocation data be collected? ■ If yes, will it be inherently identifiable or identifiable in conjunction with other data from the participant? ○ Will audio or video recording be passively collected? ■ If yes, will participants be notified when passive audio or video data collection is occurring (e.g. a "recording" light on their device will be turned on when the camera is collecting video data)? ○ Are there privacy risks for non-participant third-parties implicated by the types of data collection proposed (e.g. passive video or audio capture)? ■ If yes, has the IRB considered the risks to third-parties in their risk-benefit assessment? ■ Are the risks sufficient to require third-party consent to the research? • Data management ○ Will data sets be coded, de-identified, or otherwise dissociated from participant identifiers? ○ How will the data be stored (e.g. using network attached storage, on an external hard drive, and in the cloud)? ■ Is the data encrypted when stored? ○ How will the data be transferred? ■ Is the data encrypted when transferred? ○ With whom will the data be shared, and in what form? ■ If data will be shared beyond the research team in identifiable form, are the objectives of this secondary use clearly described? Are the risks to participants outweighed by the benefits? ○ Do any third-parties (e.g. device manufacturer, software manufacturer, and backend data collector) have access to and/or control over research data? • Will participants be asked to agree to Terms of Use, End-User License Agreements, and/or Privacy Policy statements? ○ If yes, does acceptance of these policies grant the developer of these technologies or other party's permission to view and/or share data? ○ If yes, do they contain exculpatory language? • Are the privacy and confidentiality risks clearly disclosed to participants in consent materials? Including: ○ The types of active and passive data collection that will take place. ○ Any data collection extraneous to the research, including personal data that applications

(continued)

Table 1. Continued

Category	Points to consider
	downloaded to personal devices will access. ○ Whether and what types of geolocation data will be collected (e.g. continuous location tracking or location at discrete time points). ○ The privacy and confidentiality risks contained in Terms of Use, End-User License Agreements, and/or Privacy Policy statements and clarification that participants do not waive legal rights by participating in the study. ○ Plans for sharing data for future use and in what form (i.e. identifiable or de-identified). ○ Risks of data breach and re-identification.
Monitoring and the expectation of care	• Will a mHealth technology be used for safety monitoring? ○ Is the technology validated or approved for this use? ○ If yes, how frequently will incoming safety data be accessed and reviewed for safety concerns? • Will the incoming safety data be accessed and reviewed by the research team, an independent monitoring committee, or both? ○ If no, do participants understand that the technology is NOT validated and will not alert to safety concerns? • If assessing the real-world impact of validated mHealth technologies, have criteria for intervening to prevent excessive risks been defined?
Returning results	• Have participants been blinded from receiving unvalidated device readings and data? • Do participants adequately understand the implications of the possibility of false positives and false negatives? • Is there a possibility that the mHealth technology might identify incidental findings? ○ If yes and those findings will be returned directly to participants via the mHealth platform, have participants been alerted to this possibility and counseled on when and how to access follow-up support? ○ If yes and the findings will not be returned directly to participants but to the research team, is the protocol clear on the conditions under which results will be returned to participants and plans for facilitating follow-up?
Justice and access	• Is it possible to provide a device issued by the study team for the duration of the study? • Is any population unnecessarily excluded from the research, device, platform, or mHealth intervention? • Does the study team intend to offer training to all participants on how to use the mHealth platform and/or device effectively? ○ If yes, will individuals be made aware of this training prior to enrollment? • Does the study team intend to provide ongoing technical support throughout the study? ○ If yes, will individuals be made aware of this technical support prior to enrollment? • If the research is evaluating a mHealth intervention, is it likely that the research population will be able to access this intervention after the research has concluded? ○ If no, will the research team invite participants to retain possession of the mHealth technology upon completion of their participation in the research?

information on data quality assurance methods and the names, credentials, and affiliations of the parties who have access to the data.[26]

IRBs should be especially vigilant in assessing the scientific value of mHealth studies, taking pains to ensure that the study question has not been previously addressed and that answering the question stands to advance knowledge in some meaningful way. IRBs should also pay close attention to the data and statistical plan, requiring that a principled approach to analysis be clearly stated in study materials and seeking outside statistical expertise as needed. IRBs should also ensure that the protocol is clear about plans for excess data and any secondary data uses and that confidentiality measures are in place, including adequate disclosure of data usage plans in consent materials.

Standards for public reporting of mHealth data and study results, both in academic journal and public registries, should be the same for mHealth as non-mHealth research. MHealth researchers have an obligation to report on whether their objectives, including any exploratory objectives, have been met and how this was determined. As with other types of research, we do not believe that mHealth researchers have an obligation to report on data not used to assess the study objectives articulated in the protocol. Whether or not mHealth studies are legally required to register with public platforms such as clinicaltrials.gov will depend on the nature of the study and whether they meet the public reporting criteria set out by regulators or journal editors. When public reporting is required by applicable regulations, IRBs should request a clear statement

from sponsors acknowledging this obligation and stating their intent to comply with it in the study protocol and/or consent materials. However, even when not required as a matter of regulations or publication, registering on public platforms is supported by the ethical aims of transparency and improving public trust in research.

Privacy and confidentiality

Passive data collection is unique to mHealth research and raises novel privacy issues. Not all of the voluminous and fine-grained biological, behavioral, and social information collected by mHealth devices may be related to the research.[27–29] This includes location tracking, which has significant ethical implications.[30,31] Some forms of location tracking only permit inferences about patterns of movement relative to different points without permitting inferences about the whereabouts of those points. Others, such as the smartphone platform used by researchers at the MIT Media Lab to study social distancing in New York City during the COVID-19 pandemic, track and keep an anonymized record of a user's actual geographic locations.[32] Even if such data sets are coded and do not contain direct identifiers (such as name or zip code), they may permit inferences about a user's place of residence and movements, and thus their identification, relatively easily, especially in cases where other data collected from the same device are accessible.[33]

In addition to location, and as noted earlier, mHealth may also passively collect audio and video data. On smart devices, the microphone and audio data capture enable the use of voice commands to bots such as Siri or Alexa. Similarly, video data collection may be enabled for such purposes as facial recognition for unlocking a device or monitoring the motor skills and movements of individuals. Passive audio and video capture raise risks not only for users of mHealth devices, but for third-parties as well, who may become the object of audio and video recording without their own knowledge or consent.[17,34,35]

Passive data collection risks arise both when devices are provided to study participants, given the potential for devices to come pre-configured with certain default settings, as well as when participants are asked to download mobile apps to their own personal devices. Some applications may embed, in the download agreement, permission to access data stored on one's personal device that are not connected to research participation, such as personal contacts, purchase history, or location, as well as camera and microphone. These data may be used in a variety of ways, including being disclosed to regulatory and legal authorities at their request, or because of state reporting requirements, or sold for marketing or other purposes.[22] While the details of such collection and use are typically disclosed in Privacy Policies and Terms of Use, empirical research has shown that a vanishingly small number of people read such disclosures.[36] Failure to alert individuals to the risks embedded in Privacy Policies and Terms of Use may prevent adequate informed consent. Moreover, while participants may have already agreed to these statements if using their own device and a common platform (such as, e.g., Zoom or FaceTime), their research use may involve the disclosure and transfer of sensitive information that was not envisioned at the time of initial agreement. It should not be assumed that users of these technologies are sufficiently informed of their research risks simply because they are stated in Term of Use or Privacy Policy agreements.

Relatedly, Privacy Policies and Terms of Use often function to restrict and limit liability of software developers and require users to waive certain rights. Insofar as agreeing to these documents is required for study participation, they may thereby conflict with the regulatory prohibition against exculpatory language in consent materials, a view supported by US regulatory guidance.[15,37] This presents challenges for any research use of mHealth subject to Common Rule or Food and Drug Administration (FDA) regulations that requires participant agreement with such statements.

While the risks present in these agreements should not generally deter the use of mHealth in research, IRBs should be sensitive to their presence and the content of these agreements generally, assessing their risks and exploring mitigation strategies in the context of specific studies. In cases where the research sponsor has control over the content of Privacy Policy or Terms of Use agreements, IRBs should make efforts to convince the manufacturer to alter this component of the software, insofar as it is not essential to assessing study objectives, and remove any exculpatory language embedded in the agreements. In the more common cases where researchers do not have control over the content of the agreements, IRBs should at least require disclosure of exculpatory language and the risks of these agreements generally in consent documents.[38]

The confidentiality risks of research involving mHealth technologies run parallel to the privacy risks and stem from the potential for data collected, transmitted, and stored via mHealth platforms to be inadvertently leaked or intentionally breached.[34] Inadvertent data disclosure to third-parties poses the potential for discrimination (such as the possibility of employment discrimination when a person's disease status is inadvertently disclosed) as well as legal risks (such as the possibility of an undocumented immigrant's immigration status being leaked). These risks

are heightened when data are shared for purposes unrelated to the research for which they were originally collected; such secondary uses of data should always be clearly disclosed to participants. Sponsors and investigators should also take pains to ensure adequate substantive confidentiality protections, the strength of which should vary with the degree of sensitivity of the data and can range from requiring data encryption, complying with accepted standards for secure data transfer (e.g. those found in the General Data Protection Regulation or Health Information Technology for Economic and Clinical Health Act), and, in the United States, obtaining a certificate of confidentiality for federally funded and/or FDA regulated research. IRBs should review for these protections and ensure adequacy, keeping in mind that they may seek outside expertise on data security when needed, as permitted by the regulations.[39]

Monitoring and the expectation of care

One familiar requirement of clinical research is the duty to monitor study participants to ensure safety and ongoing adverse event collection.[40,41] Instead of relying on site visits and face-to-face procedures with study staff, mHealth technologies may themselves be leveraged to accomplish safety monitoring, itself a potentially attractive feature of mHealth research. However, this may also give rise to distinct ethical and practical challenges concerning when and how best to initiate safety follow-up and the extent of the research team's "duty to rescue."[33]

Ethical issues associated with monitoring for mHealth studies vary and depend on the nature of the research. For studies attempting to validate mHealth interventions, participants may simultaneously engage with a second, already validated mHealth platform. For example, a study may ask participants to wear both a validated and an unvalidated continuous glucose monitor. In such cases, there should be regular monitoring of the source of validated results so that appropriate follow-up can be initiated if participants are at risk or in crisis. This can be self-monitoring on the part of participants, who may be instructed to respond appropriately to incoming warning signals, but periodic monitoring by the research team or another third-party (such as a clinician or the participant's primary care provider) is also advisable. In general, the minimum acceptable frequency and timing and overall percentage of data monitored in remote monitoring for mHealth studies should be similar to what would be deemed adequate for in-person studies. What differs for remote monitoring in mHealth studies need not be the timing or the intervals at which incoming data is monitored, or the amount of data monitored, but rather the medium by which the monitoring takes place.[42] Of course, insofar as mHealth studies collect more data points for analysis than non-mHealth studies, the monitoring plan should reflect this with more or more frequent monitoring. In most cases, delaying access to a validated source of data until the end of the study is ethically questionable and discordant with what would be expected in face-to-face studies, where some ongoing monitoring during the study is standard. That said, we acknowledge there may be situations, such as mHealth research involving healthy subjects, where blinding until study completion may, on a case-by-case basis, be justifiable.

Studies evaluating real-world health effects of *validated* mHealth tools raise different challenges. For example, a study may examine how an individual's use of an mHealth technology that is validated for measuring glucose levels in real time affects medication adherence, healthy eating habits, exercise, appropriate medical follow-up, and the like. In such studies, which typically involve notifications being sent to participants to encourage healthy behaviors, the assumption of equipoise requires researchers to remain neutral about whether the mHealth intervention will promote better outcomes. However, researchers who have ongoing access to—and attend to—the validated mHealth results may know, for example, when a participant's glucose level or blood pressure is dangerously low or high. This raises questions about the threshold for determining when the risks of remaining neutral become too high; that is, when equipoise has been disturbed and researchers become negligent, or run afoul of a duty to rescue, by failing to intervene to prevent harms to participants.

In its basic form, this dynamic is present in other contexts as well, including most interventional trials with control arms, where it is possible for a participant's therapeutic situation to worsen during participation. At the level of the individual, this is best addressed through careful specification of individual withdrawal criteria designed with preserving safety in mind. More generally, researchers should be thoughtful about proposing endpoints that permit meaningful evaluation of study objectives that cohere with the scope of their obligations to preserve participant safety and consider enlisting a data monitoring committee with access to unblinded incoming data that can make independent judgments about ongoing equipoise during the study.

Return of results

Participant interaction with *un*validated mHealth platforms and results raises distinct challenges. mHealth platforms are typically designed to interact directly with their users and provide health information in real time.

While there is evidence that participants desire greater access to research results,[43] and mHealth platforms may facilitate participant engagement in this regard, caution is needed when the platform and results are unvalidated. Providing unvalidated research results directly to participants carries the risk of type 1 (false positive) and type 2 (false negative) errors and biasing the data.

Type 1 errors may cause needless anxiety, stress, requests for medical care, and the like. They may also desensitize participants to true positives from validated sources, which may raise safety concerns. Type 2 errors, by contrast, may lead to an unjustified sense of participant complacency and security, such as a belief that one need not be compliant with their standard medical care or may put off scheduled physician visits because they are not receiving warning alerts from a mHealth device. In both cases, unjustified beliefs about one's health state may impact behavior and the study data in undesirable ways.[22] Because of this possibility, participants should ideally be blinded from receiving unvalidated results during the study. However, this is not always straightforward as many of these devices are designed to provide updates and readings to their users. Blinding participants may require special modification to the platform (e.g. disabling or obscuring display screens). In addition to rendering the platform less attractive, this may also remove a main motivation for using them, as the potential for receiving health updates in real time may be perceived by participants as a primary benefit of mHealth platforms. At the least, informed consent documents should clearly warn against the potential for type 1 and 2 errors and urge against making behavioral or medical decisions on the basis of the unvalidated results.

Participant interaction with validated mHealth platforms can also raise challenges when the platforms identify and report incidental findings unconnected to study objectives directly to participants. For example, a research participant wearing an Apple Watch to monitor the number of calories they burn per day may unexpectedly receive a notification that the wearable detected an irregular heart rhythm. Researchers should anticipate incidental finding data that may be shared directly with the participant and disclose to participants which results they might expect to receive, making themselves available for advice and referral for appropriate follow-up when needed. In cases where incidental findings are not returned directly to participants via mHealth devices but are accessible to the study team, the protocol should lay out the conditions under which the findings will be communicated to participants. In general, researchers have an obligation to facilitate return of medically actionable incidental findings when doing so will or may permit the prevention of significant harm to participants, in conformity with ethical guidelines for returning incidental findings in research generally.[44] IRBs should ensure that protocol plans are acceptable in this regard and that plans for returning incidental findings are adequately disclosed in consent materials.

Justice and access

While the convenience of mHealth technologies has the potential to improve access to research generally, some groups, such as the economically vulnerable, may still lack access to these technologies while other groups, such as the elderly, may lack the technological knowledge and savvy needed to effectively use them.[34] This raises broad questions of justice concerning whether the opportunities and benefits of mHealth research participation will be distributed fairly among societal groups or rather reinforce existing disparities.

The most equitable practice for mHealth studies is to avoid requiring participants to supply their own device as a condition of participation and rather offer to provide a study-issued device at no cost for the duration of participation, with software enabling translation for non-English speakers. The study-issued device should be configured in a way that minimizes the aforementioned privacy and confidentiality risks, as we outline in Table 1. In addition, training should be offered to all participants at enrollment and ongoing technical support provided throughout the study to help them understand and effectively use the platform. Individuals should be made aware of this technical support prior to enrollment so that those who lack technological knowledge are not dissuaded from participation.

Researchers should be cognizant of whether the populations enrolled in research that evaluate mHealth interventions are likely to be able to access these interventions after the research has concluded. Excluding these populations from research would only reinforce disparities in digital access. A more equitable solution would be to invite participants to retain possession of the mHealth technology once their participation in the research is complete. Such offers may be made at the time of consent, may count as a benefit capable of compensating participants for the time-commitment and burdens they undertake as part of their participation, and may also function to incentivize study completion. While IRBs should assess the potential for such benefits to unduly influence decisions to participant, in general, such incentives can both promote fairness for participants and increase access to research, by acknowledging the costs of research participation and helping to overcome them.[45]

Conclusion

Mobile health technologies hold the potential to decentralize clinical research, empower participants, and

increase efficiency. In the time of COVID-19 and other public health emergencies, they also carry significant public health benefits, enabling research to continue at a time when the public health risks of face-to-face interaction might otherwise foreclose it. While the use of mHealth in research presents distinctive ethical challenges warranting sustained attention within the research community, in many cases there are levers for mitigating the risks. We present these in Table 1 as points-to-consider that can enable sponsors, investigators, and IRBs to confidently and ethically design, implement, and review research uses of mHealth technologies.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD


Luke Gelinas https://orcid.org/0000-0002-6277-148X

References

1. Marra C, Chen JL, Coravos A, et al. Quantifying the use of connected digital products in clinical research. *NPJ Digit Med* 2020; 3: 50.
2. U.S. Food and Drug Administration. *Digital health policies and public health solutions for COVID-19*, https://www.fda.gov/medical-devices/coronavirus-covid-19-and-medical-devices/digital-health-policies-and-public-health-solutions-covid-19 (2020, accessed 28 April 2021).
3. U.S. Food and Drug Administration. Enforcement policy for non-invasive remote monitoring devices used to support patient monitoring during the coronavirus disease 2019 (COVID-19) public health emergency (revised), 2020, https://www.fda.gov/regulatory-information/search-fda-guidance-documents/enforcement-policy-non-invasive-remote-monitoring-devices-used-support-patient-monitoring-during
4. U.S. Food and Drug Administration. Remote or wearable patient monitoring devices EUAs, https://www.fda.gov/medical-devices/coronavirus-disease-2019-covid-19-emergency-use-authorizations-medical-devices/remote-or-wearable-patient-monitoring-devices-euas?utm_campaign=2020-06-18%20New%20EUA%20COVID-19%20page&utm_medium=email&utm_source=Eloqua (2020, accessed 28 April 2021).
5. U.S. Food and Drug Administration. Coronavirus treatment acceleration program (CTAP), https://www.fda.gov/drugs/coronavirus-covid-19-drugs/coronavirus-treatment-acceleration-program-ctap (2021, accessed 28 April 2021).
6. Mather N. How we accelerated clinical trials in the age of coronavirus. *Nature* 2020; 584: 326.
7. Budd J, Miller BS, Manning EM, et al. Digital technologies in the public-health response to COVID-19. *Nat Med* 2020; 26: 1183–1192.
8. Scott BK, Miller GT, Fonda SJ, et al. Advanced digital health technologies for COVID-19 and future emergencies. *Telemed J E Health* 2020; 26: 1226–1233.
9. Adans-Dester CP, Bamberg S, Bertacchi FP, et al. Can mHealth technology help mitigate the effects of the COVID-19 pandemic? *IEEE Open J Eng Med Biol* 2020; 1: 243–248.
10. Nachega JB, Leisegang R, Kallay O, et al. Mobile health technology for enhancing the COVID-19 response in Africa: a potential game changer? *Am J Trop Med Hyg* 2020; 103: 3–5.
11. Wittbold KA, Carroll C, Iansiti M, et al. How hospitals are using AI to battle COVID-19. *Harvard Business Review*, 3 April 2020, https://hbr.org/2020/04/how-hospitals-are-using-ai-to-battle-covid-19
12. Pew Research Center. Mobile fact sheet, https://www.pewresearch.org/internet/fact-sheet/mobile/ (2021, accessed 28 April 2021).
13. Pew Research Center. Smartphone ownership is growing rapidly around the world, but not always equally, https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/ (2019, accessed 28 April 2021).
14. Kakkar AK, Sarma P and Medhi B. MHealth technologies in clinical trials: opportunities and challenges. *Indian J Pharmacol* 2018; 50: 105–107.
15. Nebeker C, Wilbanks JT and Rothstein MA. MHealth research applied to regulated and unregulated behavioral health sciences. *J Law Med Ethics* 2020; 48: 49–59.
16. Nebeker C, Murray K, Holub C, et al. Acceptance of mobile health in communities underrepresented in biomedical research: barriers and ethical considerations for scientists. *JMIR Mhealth Uhealth* 2017; 5: e87.
17. Nebeker C, Harlow J, Espinoza Giacinto R, et al. Ethical and regulatory challenges of research using pervasive sensing and other emerging technologies: IRB perspectives. *AJOB Empir Bioeth* 2017; 8: 266–276.
18. Gerke S, Shachar C, Chai PR, et al. Regulatory, safety, and privacy concerns of home monitoring technologies during COVID-19. *Nat Med* 2020; 26: 1176–1182.
19. Nebeker C, Torous J and Ellis RJB. Building the case for actionable ethics in digital health research supported by artificial intelligence. *BMC Med* 2019; 17: 137.
20. 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: 577–586.
21. Segura Anaya LH, Alsadoon A, Costadopoulos N, et al. Ethical implications of user perceptions of wearable devices. *Sci Eng Ethics* 2018; 24: 1–28.
22. Rothstein MA, Wilbanks JT, Beskow LM, et al. Unregulated Health research using mobile devices: ethical considerations and policy recommendations. *J Law Med Ethics* 2020; 48: 196–226.
23. U.S. Department of Health and Human Services Office for Human Research Protections. *OHRP guidance on coronavirus*, https://www.hhs.gov/ohrp/regulations-and-policy/

guidance/ohrp-guidance-on-covid-19/index.html (2020, accessed 28 April 2021).
24. U.S. Food and Drug Administration. *FDA guidance on conduct of clinical trials of medical products during the COVID-19 pandemic*. Silver Spring, MD: U.S. Food and Drug Administration, 2020.
25. Coran P, Goldsack JC, Grandinetti CA, et al. Advancing the use of mobile technologies in clinical trials: recommendations from the Clinical Trials Transformation Initiative. *Digit Biomark* 2019; 3: 145–154.
26. Eysenbach G. CONSORT-EHEALTH: improving and standardizing evaluation reports of web-based and mobile health interventions. *J Med Internet Res* 2011; 13: e126.
27. Booth BM, Mundnich K, Feng T, et al. Multimodal human and environmental sensing for longitudinal behavioral studies in naturalistic settings: framework for sensor selection, deployment, and management. *J Med Internet Res* 2019; 21: e12832.
28. Mok TM, Cornish F and Tarr J. Too much information: visual research ethics in the age of wearable cameras. *Integr Psychol Behav Sci* 2015; 49: 309–322.
29. Nebeker C, Linares-Orozco R and Crist K. A multi-case study of research using mobile imaging, sensing and tracking technologies to objectively measure behavior: ethical issues and insights to guide responsible research practice. *J Res Adm* 2015; 46: 118.
30. Fuller D, Shareck M and Stanley K. Ethical implications of location and accelerometer measurement in health research studies with mobile sensing devices. *Soc Sci Med* 2017; 191: 84–88.
31. Calvo RA, Deterding S and Ryan RM. Health surveillance during covid-19 pandemic. *BMJ* 2020; 369: m1373.
32. Bakker M, Berke A, Groh M, et al. Social distancing in New York City. Medium, 30 March 2020, https://medium.com/mit-media-lab/social-distancing-in-new-york-city-a27340532931
33. Jacobson NC, Bentley KH, Walton A, et al. Ethical dilemmas posed by mobile health and machine learning in psychiatry research. *Bull World Health Organ* 2020; 98: 270–276.
34. Carter A, Liddle J, Hall W, et al. Mobile phones in research and treatment: ethical guidelines and future directions. *JMIR Mhealth Uhealth* 2015; 3: e95.
35. Eyal N, Kimmelman J, Holtzman LG, et al. Regulating impact on bystanders in clinical trials: an unsettled frontier. *Clin Trials J* 2019; 16: 450–454.
36. Obar JA and Oeldorf-Hirsch A. The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services. *Inf Commun Soc* 2020; 23: 128–147.
37. U.S. Food and Drug Administration. Guidance on exculpatory language in informed consent, 2011, https://www.hhs.gov/ohrp/regulations-and-policy/requests-for-comments/guidance-exculpatory-language/index.html
38. Secretary's Advisory Committee on Human Research Protections. Attachment B—clarifying requirements in digital health technologies research, 2020, https://www.hhs.gov/ohrp/sachrp-committee/recommendations/april-7-2020-attachment-b/index.html
39. 45 C.F.R. § 46.107e (2021).
40. 21 C.F.R. § 56.111a(6) (2021).
41. 45 C.F.R. § 46.111a(6) (2021).
42. Gelinas L and Riddle J. Accelerating the recovery—design and IRB review of safety monitoring plans during COVID-19. *Advarra*, 3 August 2020, https://www.advar ra.com/blog/accelerating-the-recovery/ (accessed 28 April 2021).
43. The National Academics of Sciences, Engineering, and Medicine. Principles for the return of individual research results: ethical and societal considerations. In: Botkin JR, Mancher M, Busta ER, et al. (eds) *Returning individual research results to participants*. Washington, DC: The National Academies Press, 2018, pp. 59–92.
44. The Multi-Regional Clinical Trials Center of Brigham and Women's Hospital and Harvard. Return of individual results to participants recommendations document, version 1.2, 2017, https://mrctcenter.org/wp-content/uploads/2017/12/2017-12-07-Return-of-Individual-Resullts-Recommendations-Document-V-1.2.pdf
45. Gelinas L, White SA and Bierer BE. Economic vulnerability and payment for research participation. *Clin Trials J* 2020; 17: 264–272.