Chapter 12
ICT and Mobile Data for Health Research

David Coles, Jane Wathuta and Pamela Andanda

Abstract Mobile cellular subscriptions had reached 87% of the world's population by 2011 (ITU 2011). Notably, Africa has "the fastest mobile phone growth rate in the world and … a proliferation of social media users" (Mutula in Information ethics in Africa: cross-cutting themes. African Centre of Excellence for Information Ethics, Pretoria, pp 29–42, 2013:31). Mobile phones that can run software applications (apps) are increasingly used in health settings, for example, to improve diagnosis and personalize health care (Mosa et al. in BMC Medical Informatics and Decision Making 12(1):67, 2012). This fast-paced development saw the number of "mHealth" apps reach 97,000 as of March 2013 (He et al. in AMIA Annual Symposium Proceedings, pp 645–654, 2014).

Keywords Health research · ICT · mHealth · Mobile data · Mobile phones Personal data

The application of mobile technologies (mobile phones or other remote monitoring devices) for health-related purposes is termed "mHealth": a mobile tool for expanding access to health information and services around the world (K4Health 2014). According to the World Health Organization (WHO 2011:6) , mHealth is the "medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants and other wireless devices". Although mHealth has come to signify the use of any mobile technology to address health care challenges such as access, quality, affordability, matching of resources and behavioural norms (Qiang et al. 2011), most mHealth interventions use mobile phone technology, thanks to its versatility as an ICT tool (Leon and Schneider 2012:7).

D. Coles (✉)
University of Central Lancashire, Centre for Professional Ethics, The Bacchus House, Elsdon, Newcastle upon Tyne NE19 1AA, UK
e-mail: david.coles@hazyrays.com

J. Wathuta · P. Andanda
University of the Witwatersrand, Private Bag 3 Wits, Johannesburg 2050, South Africa

D. Schroeder et al. (eds.), *Ethics Dumping*, SpringerBriefs in Research and Innovation Governance, https://doi.org/10.1007/978-3-319-64731-9_12

With the pervasive growth in technology infrastructure, mHealth can reach communities in ways that conventional health services and other communication tools cannot. Mobile phones are described as potentially the most widespread embedded surveillance tools, especially due to the use of location sensors and the consequent possibility of documenting and quantifying habits, routines, and personal associations (Shilton 2009). This case study focuses on the potential ethical issues associated with the use of mHealth apps in medical research and health care. mHealth offers "attractive low-cost, real-time ways to assess disease, movement, images, behaviour, social interactions, environmental toxins, metabolites" (Collins 2012:1). It has the power to bring the research lab to the patient and obtain real-time, continuous biological, behavioural and environmental data (Collins 2012).

Mobile phones collect a wide range of personal information from their users, with or without their knowledge, which raises novel and complex ethical and practical challenges. Research teams (and clinicians) need to understand these challenges so that, without rejecting mHealth and related mobile technological advancements, they minimize any unintended harms (Carter et al. 2015). Wicklund (2015) observes that clinical studies that utilize mHealth devices and platforms are venturing into uncharted ethical territory.

Area of Risk of Exploitation

Software apps in the mHealth category can be used for collecting health-related data on a large scale for biomedical research; the so-called "big data" (Park and Jayaraman 2014; Hsieh et al. 2013). In general, however, mHealth raises concerns regarding data security issues – from transmission of data to its local storage, and "ownership" of what is otherwise considered confidential patient data. This data is easy to obtain, but difficult or impossible to retract once shared. In addition to safety and security risks, mobile sensing also disrupts social boundaries and challenges distinctions between public and private (Shilton 2009). One of the key challenges of using mHealth in low- and middle-income countries (LMICs) is how to ensure workable approaches to privacy and security (Leon and Schneider 2012:19).

Carter et al. (2015) have identified a range of ethical issues raised by the use of mobile phones for research and clinical purposes. These are:

- the protection of privacy
- minimizing third-party uses of data
- informing patients of complex risks when obtaining consent
- maximizing benefits while minimizing the potential for disclosure to third parties
- care in the communication of clinically relevant information
- the rigorous evaluation and regulation of mHealth products before widespread use

In practical terms, the issues discussed below need to be considered carefully.

Context-Based and Fully Informed Consent Should Be Obtained

Researchers should seek and obtain informed consent before using mHealth technologies in research. Accordingly, participants must be informed about, and understand the risks and benefits of, mHealth technologies, and then make a free and voluntary decision to participate or not. The risks associated with mHealth are complex, and these need to be communicated and negotiated. If the study involves the collection of data from interaction with identifiable third parties, it may be necessary to obtain their informed consent as well. This in turn means that mHealth participants will have to disclose their condition and/or mHealth participation (Carter et al. 2015).

Only Necessary Data Should Be Collected

Compared with other health information systems, mHealth collects a much larger amount and broader range of data about patient lifestyles and activities, over an extended period (He et al. 2014). A potential danger to bear in mind in this regard is that of collecting excessive amounts of raw data to maximize the information extracted by the research team (Carter et al. 2015).

Any Tracking Should Be Proportionate and the Correct Person Should Be Tracked

Continuous or intermittent recording and transmission of detailed information about where a person is, and to some extent what they are doing, may breach privacy and confidentiality. There are risks of inadvertent insight into a participant's behaviour revealing information beyond the profiles that are scientifically justified and for which data collection was employed. This also poses problems of informed consent, as privacy may be violated in ways unforeseen by either investigators or participants. Text messages (SMS) can be read by persons other than the intended recipient; messages can be forwarded and can remain on unsecured devices indefinitely. One result could be the unintended disclosure of a medical condition (Labrique et al. 2013).

Research Participants Should Know Exactly Which Data Is Collected and Who Will or Could Have Access to It

This is a great challenge, especially in a global research environment that increasingly requires the sharing of data in publicly available repositories. The case of an alleged breach of smartphone users' privacy by manufacturers of popular smartphone apps for Apple and Android devices illustrates this risk. The manufacturers are alleged to have gathered information from personal address books on the phones of Kenyan users, stored it on their own computers, and transmitted it without the knowledge of its owners, all of which demonstrates how difficult it is to guarantee privacy when using smartphones (Mutula 2013; Wambugu 2012).

The security of data collected via mobile phones cannot be guaranteed either, in part because no strict privacy regulations exist.[1] Many mHealth apps do not use encryption when transferring data, and even when they do, hackers and governments can still gain access. Potential violations of privacy include hacking of personal data with the known likelihood of identity theft and financial losses, computer malware and virus programs, and malevolent apps planted by developers who steal data for commercial or criminal purposes (He et al. 2014).

Incentives to Take Part in Research Should Be Proportionate and not Result in Exploitation

Research involving mHealth apps often requires the participant to have a smartphone. If researchers specifically target those who do not already own newer devices or other modes of mobile technology, the prospect of being given access to such technology may unduly influence them to take part (Labrique et al. 2013:3). Patients should not, however, be excluded from mHealth monitoring benefits if they cannot afford a device capable of supporting the app or connect with networks capable of transmitting potentially large volumes of data. This requirement therefore needs very careful judgement.

[1]Companies like Apple and Google have to comply with the privacy regulations in each of the countries where they collect data. Where little or no privacy regulation exists, the companies have wide scope regarding what data they collect and how they use it. Interestingly, Apple announced that with their new iOS10 operating system they would be introducing "differential privacy", which they claimed would enable them to collect much more personal user data while preserving users' privacy. This concept involves introducing numerical "noise" into the data collected in order to de-identify it (see Brandom 2016). However, it is questionable whether data provided this way will be suitable for research purposes (see Friedman and Schuster 2010).

Specific Case and Analysis

The details of a case of HIV/AIDS tele-counselling in South Africa were obtained from an interview with Cell-Life's general manager, Peter Benjamin, conducted and published in 2011 by Boyle (2011). Additional information is available in a report that was prepared on the use of mobile technologies for the monitoring and evaluation of public sector community-based health services (Leon and Schneider 2012).[2]

Cell-Life, a non-profit organization, entered into a contract with the South African national Department of Health (DOH) for a big project. "Cell-Life started in 2001 as a research collaboration between staff of the engineering faculty of the University of Cape Town (UCT) and the Cape Peninsula University of Technology (CPUT)" (Loudon and Rivett 2013). It became a not-for-profit organization in 2006 (Loudon and Rivett 2013). In terms of the contract, the DOH set up a national mHealth system that used cellphones for monitoring an HIV counselling and testing (HCT) campaign.

Cell-Life used chat software called Mxit, which enabled users to send instant messages over a cellphone system. To do this, users had to download a small app that connected them to the Mxit server, enabling immediate communication with anyone else on Mxit. The app sent SMS-type messages through GPRS,[3] via which messaging was effectively free.

Cell-Life created a website within Mxit where it provided all the usual HIV content, information and interactive quizzes. An interesting feature that Cell-Life included was linking Mxit to South Africa's National AIDS Helpline, so that users could text on Mxit and the message would go through to the computer screen of a professional HIV counsellor at the National AIDS Helpline. The counsellor would type a reply which would appear on the user's cellphone screen.

Cell-Life was awarded additional contracts by the DOH for the design and implementation of a mobile monitoring and reporting system for the national HIV counselling and testing (HCT) campaign, and the national antiretroviral treatment expansion programme (Cell-Life nd). These systems have been the subject of research into how software applications for the monitoring and evaluation of community-based care are used in a research and service delivery context (Leon and Schneider 2012).

The data processed and transmitted through the software apps related to patients' personal information, which was subsequently stored and monitored through the system. The use of mobile phones in this process raises practical ethical issues, such as concerns about the protection of information and privacy, and consent to the potential use of such information for research purposes. As Labrique et al. (2013)

[2]See also Cell-Life (nd).

[3]"General Packet Radio Service (GPRS) is a packet oriented mobile data service on the 2G and 3G cellular communication system's global system for mobile communications (GSM)" (General Packet Radio Service 2017).

have observed, although mHealth apps ensure the availability of real-time data that brings with it new and beneficial strategies, the rapid adoption of these technologies raises ethical issues that need careful consideration. Accordingly, existing standards and practices have to be supplemented with new guidelines to ensure that patients and vulnerable populations are adequately protected. The gap between technological innovation and the development of ethical standards and guidance needs to be reduced, so that researchers and other stakeholders have a reference framework for assessing and mitigating the risks of mHealth research and data collection.

Recommendations

The following measures could help avert the possibility of exploitation in the context of mHealth:

- Developers should determine when, where and how sensitive data are uploaded and stored, to minimize the risk of privacy violations. In addition, they should take steps, by using encryption and anonymization (Carter et al. 2015; He et al. 2014), to ensure that data collected by an mHealth app are not available to other apps or programs installed on the phone or in third-party storage without security and privacy guarantees (He et al. 2014).
- Participants should be able to control what they consent to and how their data may be used and stored. The data should be deleted as soon as no longer needed (Albrecht and Fangerau 2015).
- Appropriate regulation of mHealth devices and apps should be developed to ensure their safety and effectiveness, including minimal privacy violations and guarantees that they provide clinically accurate information. Albrecht and Fangerau (2015), for instance, have recommended the transformation of the fundamental principles of medical ethics in order to make them applicable to mHealth.
- Proven innovations for the improvement of data protection and privacy should be implemented by researchers as soon as possible after they become available.

References

Albrecht U-V, Fangerau H (2015) Do ethics need to be adapted to mHealth? Studies in Health Technology and Informatics 213:219–222

Boyle C (nd) (2011) mHealth benefits: little evidence – yet (2011) http://www.mobilethinkers.com/2011/01/mhealth-benefits-no-evidence-%E2%80%93-yet/

Brandom R (2016) This is what Apple's differential privacy means for iOS 10. The Verge, 17 June. http://www.theverge.com/2016/6/17/11957782/apple-differential-privacy-ios-10-wwdc-2016

Carter A, Liddle J, Hall W, Chenery H (2015) Mobile phones in research and treatment: ethical guidelines and future directions. JMIR mHealth and uHealth 3(4): e95

Cell-Life (nd) Mobile ME for the national HIV counselling and testing campaign. http://www.cell-life.org/projects/health-care-and-testing/

Collins F (2012). The real promise of mobile health apps: mobile devices have the potential to become powerful medical tools. Scientific American 307(1):1

Friedman A, Schuster A (2010) Data mining with differential privacy. In: Proceedings of the 16th ACM SIGKDD international conference on knowledge discovery and data mining. Association for Computing Machinery, New York, p 493–502

General Packet Radio Service (2017) Wikipedia: The Free Encyclopedia. Wikimedia Foundation Inc. https://en.wikipedia.org/wiki/General_Packet_Radio_Service

He D, Naveed M, Gunter CA, Nahrstedt K (2014) Security concerns in Android mHealth apps. AMIA Annual Symposium Proceedings 645–654

Hsieh J-C, Li A-H, Yang C-C (2013) Mobile, cloud, and big data computing: contributions, challenges, and new directions in telecardiology. International Journal of Environmental Research and Public Health 10(11):6131–6153

ITU (2011) The world in 2011: ICT facts and figures. International Telecommunication Union. http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf

K4Health (2014) The mHealth planning guide: key considerations for integrating mobile technology into health programs. https://www.k4health.org/toolkits/mhealth-planning-guide

Labrique AB, Kirk GD, Westergaard RP, Merritt MW (2013) Ethical issues in mHealth research involving persons living with HIV/AIDS and substance abuse. AIDS Research and Treatment 2013:189645 1–6

Leon N, Schneider H (2012) MHealth4CBS in South Africa: a review of the role of mobile phone technology for monitoring and evaluation of community based health services. South African Medical Research Council, University of the Western Cape. http://www.mrc.ac.za/healthsystems/MHealth4CBSReview.pdf

Loudon M, Rivett U (2013) Enacting openness in ICT4D research. In: Smith LM, Reilly MAK (eds) Open development: networked innovations in international development. MIT Press, Cambridge MA, p 53–78

Mosa ASM, Yoo I, Sheets L (2012) A systematic review of healthcare applications for smartphones. BMC Medical Informatics and Decision Making 12(1):67

Mutula SM (2013) Ethical dimensions of the information society: implications for Africa. In: Ocholla D, Britz J, Capurro R, Bester C (eds) Information ethics in Africa: cross-cutting themes. African Centre of Excellence for Information Ethics, Pretoria, p 29–42. http://www.africainfoethics.org/pdf/ie_africa/chapter_4.pdf

Park S, Jayaraman S (2014) A transdisciplinary approach to wearables, big data and quality of life. 36th annual international conference of the IEEE engineering in medicine and biology Society, Chicago IL, p 4155–4158

Qiang CZ, Yamamichi M, Hausman V, ltman D (2011) Mobile applications for the health sector. World Bank, Washington DC

Shilton K (2009) Four billion little brothers? Privacy, mobile phones, and ubiquitous data collection. Communications of the ACM 52(11):48–53

Wambugu S (2012) Cellphone giving away your personal privacy. Daily Nation, 18 February. http://www.nation.co.ke/oped/Opinion/Cellphone-giving-away-your-personal-privacy-/440808-1330412-tdkawuz/index.html

WHO (2011) mHealth: new horizons for health through mobile technologies: second global survey on eHealth. World Health Organization, Geneva. www.who.int/goe/publications/goe_mhealth_web.pdf

Wicklund E (2015) New project to create mHealth ethics for clinical trials. mHealth Intelligence, I December. http://mhealthintelligence.com/news/new-project-to-create-mhealth-ethics-for-clinical-trials

Author Biographies

David Coles is senior research fellow at the University of Central Lancashire's Centre for Professional Ethics and a research associate at the University of Newcastle's School of Agriculture, Food and Rural Development. Previously he was joint programme manager for the European and Developing Countries Clinical Trials Partnership, as well as developing and implementing the EU system of ethics review for the EU Framework Programme.

Jane Wathuta is a postdoctoral research fellow at the School of Law, University of the Witwatersrand, Johannesburg. She previously worked with Strathmore University and the Kianda Foundation educational trust in Nairobi. She is an advocate of the High Court of Kenya and a member of the Research Ethics Committee of the Centre for Research in Therapeutic Sciences, the Kenya Medical Research Institute, South Africa's Council for Scientific and Industrial Research and the African Centre for Clinical Trials.

Pamela Andanda is a professor of law at the University of the Witwatersrand, Johannesburg. Pamela is a member of UNESCO's International Bioethics Committee, the Ethics Review Committee of Strathmore University's Center for Research in Therapeutic Sciences, and the Data and Biospecimen Access Committee of the Human Heredity and Health in Africa (H3Africa) Consortium.