CONSENSUS STATEMENT

Dos and don'ts for mHealth-based clinical support among clinicians in South Africa: Results from a 1-day workshop

L Laflamme,[1,2] MSc, PhD; **J Chipps,**[3] BSc, MPH, PhD; **D Barrett;**[4] **P Brysiewicz,**[5,6] PhD, MN; **R Duys,**[7] MB ChB, FCA (SA), MMed (Anaesth); **K Evans,**[6] MB ChB, MMed (Emerg Med); **M A Jarvis,**[5] PhD; **M Mars,**[8] MB ChB, MD; **W Stassen,**[6] BTech, MPhil (Emerg Med), PhD; **L A Wallis,**[6] MB ChB, MD, FRCEM, FCEM (SA)

[1] *Department of Global Public Health, Karolinska Institutet, Stockholm, Sweden*
[2] *Institute for Social and Health Sciences, University of South Africa, Johannesburg, South Africa*
[3] *School of Nursing, Faculty of Community and Health Sciences, University of the Western Cape, Cape Town, South Africa*
[4] *Head of Product, Healthforce, Cape Town, South Africa*
[5] *School of Nursing and Public Health, College of Health Sciences, University of KwaZulu-Natal, Durban, South Africa*
[6] *Division of Emergency Medicine, Faculty of Health Sciences, University of Cape Town, South Africa*
[7] *Department of Anaesthesia and Perioperative Medicine, Faculty of Health Sciences, University of Cape Town, South Africa*
[8] *Department of TeleHealth, College of Health Sciences, University of KwaZulu-Natal, Durban, South Africa*

Corresponding author: *L A Wallis (lee.a.wallis@gmail.com)*

Digital technologies continue to penetrate the South African (SA) healthcare sector at an increasing rate. Clinician-to-clinician diagnostic and management assistance through mHealth is expanding rapidly, reducing professional isolation and unnecessary referrals, and promoting better patient outcomes and more equitable healthcare systems. However, the widespread uptake of mHealth use raises ethical concerns around patient autonomy and safety, and guidance for healthcare workers around the ethical use of mHealth is needed. This article presents the results of a multi-stakeholder workshop at which the 'dos and don'ts' pertaining to mHealth ethics in the SA context were formulated and aligned to seven basic recommendations derived from the literature and previous multi-stakeholder, multi-country meetings.

S Afr Med J 2021;111(5):416-420. https://doi.org/10.7196/SAMJ.2021.v111i5.15400

As is the case globally, digital technologies – especially in the form of mHealth – are penetrating the South African (SA) healthcare sector at an increasing pace. SA is known to be under-resourced in terms of healthcare providers, especially at the specialist doctor level; making the best use of these limited resources is therefore a priority, and digital technologies are instrumental to that end.[1] Clinician-to-clinician diagnostic and management assistance is a field of application on the rise that reduces professional isolation and can bring benefits such as reduced unnecessary referrals, better patient outcomes and more equitable healthcare systems.[2] Use of clinician-to-clinician mHealth has proved particularly important during the COVID-19 pandemic, given movement restrictions, the risk of infection spread, and reduced clinical services. However, digital communication raises substantial ethical concerns[3-9] around the loss of privacy and self-determination inherent in how information is handled, and threats to patient safety emerging from weaknesses in the quality of the digital information deep-rooted in the iterative development process of mHealth apps. Errors and mischievous additions are silent and built in during the app development,[10,11] or result from issues such as clinical users' failure to use mHealth apps and/or devices appropriately,[11,12] or unstandardised and unsupervised environments of use.[12,13]

In this article, we report the outputs of a workshop focused on front-line use of mHealth for clinical support among healthcare workers.

The Brocher Proposition

Recognising that it is imperative to come to terms with the above ethical issues, in 2019 we held a 3-day workshop focused on image-based digital diagnostic assistance in sub-Saharan Africa, a target for mHealth applications given the many rural and hard-to-reach communities. Twenty-seven global mHealth stakeholders from diverse professional and geographical backgrounds completed a solution-orientated consensus process. The outcome was a list of actions aimed at reducing threats to autonomy, safety and justice implicit in digital technologies. The recommendations, compiled in the 'Brocher Proposition',[8] were organised and disaggregated according to the three stages of the life cycle of mHealth applications (development, implementation and scale-up). Once the detailed recommendations had been published, they were synthesised in a set of seven 'pillars' that cut across the phases of technological development and the ethical principles, namely: (*i*) Be guided by the endpoint; (*ii*) Apply straightforward clinical standards; (*iii*) Integrate into existing healthcare system; (*iv*) Seek guidance from existing regulatory frameworks; (*v*) Build in protective solutions; (*vi*) Make ethics a quality assurance measure; and (*vii*) Focus on self-determination and governance[9] (Table 1). These pillars were used as the basis for the second workshop, which we report on in this article.

Table 1. Seven pillars for ethics in digital diagnostic assistance among clinicians (from Laflamme and Wallis[9])

Pillar	Clarification
1. Be guided by the endpoint	The ultimate goal of any digital health intervention should be better health. All stakeholders involved, regardless of the competence or perspective they contribute, should bear that in mind.
2. Apply straightforward clinical standards	The gold standard for diagnosis is 'bedside' consultation; any compromises on the standard of care delivered must be avoided. Following locally agreed standards that are customised to the health system ensures that clinicians can have confidence in the guidance that is provided.
3. Integrate into existing healthcare system	Digital solutions must integrate into current practices in a seamless manner so as to avoid workflow disruption; they must therefore also be relevant in the local health system context.
4. Seek guidance from existing regulatory frameworks	It is essential that already-existing regulations and frameworks guide the development and implementation process of digital solutions in spite of the need for them to be 'locally tailored'.
5. Build in protective solutions	Stakeholders must be made aware of the potential consequences of errors. Engineers and designers should receive proper guidelines to help build solutions to mitigate the occurrence of errors.
6. Make ethics a quality assurance measure	Routine analysis and follow-up mechanisms help foresee and mitigate ethical challenges.
7. Focus on self-determination and governance	Inclusive procedures from development to scale ensure that local stakeholders – including patients themselves – can engage.

The Cape Town 'practical response': Dos and don'ts

We held a second workshop in Cape Town in December 2019 to create consensus on what should be done and not done (the 'dos' and 'don'ts') in application of digital technologies for clinician-to-clinician assistance. The scope was deliberately broadened beyond image-based digital consultation, but was focused on the SA context. The Brocher proposition 'pillars' were used as reference.

While recent legislation has addressed many issues related to privacy, data handling and storage, and record-keeping, regulatory challenges still exist in mHealth use in SA; at the time of the workshop it was anticipated that, in the medium to long term, those not yet adequately covered would be addressed by national regulatory bodies (e.g. the Office of Health Standards Compliance, Health Professions Council of South Africa, South African Nursing Council, Wireless Application Service Providers Association (self-regulatory) and South African Health Products Regulatory Agency).[14]

Participants. The participants in the workshop were professionally and geographically spread stakeholders (N=21; 12 women) working in governmental agencies (n=4), public (n=3) and private (n=5) organisations, or universities (n=9). The participants covered national and provincial spheres of government, private developers and software companies, non-governmental health applications, public health, and several clinical fields including nursing, emergency medicine and critical care. The views expressed represented participants' own views rather than those of their respective organisations.

Process. The morning was spent on the ethical principles of autonomy and privacy and the afternoon on safety. The dos and don'ts were generated through group discussions (three heterogeneous groups) and reported in plenum. Each group was assigned two group-specific pillars, and all groups discussed pillar 6, 'Make ethics a quality assurance measure'. Each group had a chair, note takers and rapporteurs. At the end of the day all notes were gathered, and during the following week, they were revisited to uniformise the style, i.e. each statement starting with a verb. Group member checks and validation took place during the following weeks, and the dos and don'ts by pillar and ethical principle were obtained in their close-to-final wording. In the case of pillar 6, addressed by all three groups, similar or overlapping answers were grouped using formulation as close as possible to the original texts. The integral version was circulated to all participants for final review and comments.

Dos and don'ts to safeguard patient autonomy – self-determination is key

Patients participating in mHealth processes, where data about them are stored on undetermined platforms for an indefinite time and eventually made available to third parties, were a major concern at the meeting. All groups agreed that, while some regulation exists in this area, more needed to be done to impede individual data being put into circulation without consent, and that a mix of straightforward and more complex dos or don'ts was necessary.

The recommendations emanating about patient autonomy evolved mainly around what could be done – or avoided – to engage patients more forcefully in processes and decisions that pertain to their health and healthcare and to build seamless yet transparent systems and processes that allow for straightforward communication and facilitate the tasks and work flow (Table 2). To 'establish patient-friendly and service-streamlined consent procedures' is therefore guided by the endpoint ('Do' in pillar 1) or consent procedures that do not interrupt the provision of care ('Don't' in pillar 5): there are similar examples in other pillars. As for pillar 6, 'Make ethics a quality assurance measure', the Dos that were put forward across the working groups touched upon state-of-the-art consent procedures, state-of-the-art data management procedures, the establishment of strong independent agencies, and the provision of guidance and support tools to all users throughout the whole process.

Dos and don'ts to safeguard patient safety – never lose track of the gold standard

Patient safety was a shared value among all stakeholders. Discussions mostly dealt with how to ensure that the clinicians involved in digital processes of consultation among colleagues would not be

Table 2. Autonomy

Pillar	Do	Don't
1. Be guided by the endpoint	• Make users aware of critical issues and establish standards for communication between provider and patient • Establish patient-friendly and service-streamlined consent procedures • Implement systems that allow for patients to easily access their whole medical records • Establish an external reporting system for patients to report confidentiality violations	• Make use of passive consent • Inhibit routine clinical practice with consent procedures
2. Apply straightforward clinical standards	• Establish uniform standards of care in accordance with those locally and internationally accepted • Provide user support tools for patient data access, use, and sharing • Provide all patients with the same standard of care	• Allow technology to replace the patient/provider interaction
3. Integrate into existing healthcare system	• Seek informed consent in all service instances • Integrate bypass function to digital systems to prevent data storage on clinicians' personal devices	• Download photos/patient information to clinicians' personal devices • Treat the digital system as different from the routine healthcare system
4. Seek guidance from existing regulatory frameworks	• Ensure that guidelines are endorsed by the related ethics regulatory body • Record digital consultation notes	
5. Build in protective solutions	• Think about levels of consent, especially when consent could interrupt care • Follow a human-centred design process • Have a tick-box to say consent was obtained • Minimise the possibility of technology downtime	• Have consent procedures that interrupt the provision of care
6. Make ethics a quality assurance measure	• Implement state-of-the-art consent procedures • Employ state-of-the-art data management procedures • Establish strong independent agencies for good system governance • Provide all users with guidance and support tools throughout the whole process • Have interoperability in mind from the onset	
7. Focus on self-determination and governance	• Provide information in clinical settings on why phones are used in consultations • Train clinicians in consent seeking • Clarify what data are being gathered about patients • Have option for patients to retract their data • Make use of context-relevant consent procedure, including appropriate language • Provide context-relevant terms and condition of usage, including appropriate language	• Make explaining data management clinicians' responsibility • Completely delete information – store it for 5 years but revoke access

distracted from the gold standard that must be at the core of every patient's care: that of face-to-face consultation and care. As shown by the Dos and Don'ts proposed under patient safety (Table 3), this gold standard must not be compromised at the expense of, for instance, large and unmotivated data collections (pillar 1), complex work processes (pillar 2) or stand-alone and disintegrated systems (pillar 3). As was the case for the safeguarding of patient autonomy, many Dos dealt with different forms of support that the users should be provided with, including built-in tools, straightforward procedures and guidelines. More Don'ts were presented and for more pillars than for patient autonomy. For pillar 3 ('Integrate into existing healthcare system'), for instance, the Don't is about not implementing systems that distract clinicians from patient care in excess of existing work processes. For pillar 6, 'Make ethics a quality assurance measure', the Don'ts centred around being careful with the assumption of knowledge: to avoid assuming that front-line clinicians know something and thereby refraining from regularly sharing expertise. The Dos were broad, ranging from aligning the choice and flow of data to patient safety requirements, to providing medicolegal support to users as needed.

Moving into practice

Digital health technologies already have an established presence in SA healthcare practice, to facilitate timely clinician-to-clinician interaction while allowing stretched front-line staff to focus on the patients at hand. COVID-19 has made this role even more important, highlighting the urgent need for an updated regulatory framework and clear ethical guidelines.

Table 3. Safety

Pillar	Do	Don't
1. Be guided by the endpoint	• Restrict the amount of data collected to the minimum essential data points • Introduce controls and authentication procedures for clinicians • Ensure that digital systems are auditable	• Collect irrelevant data • Overlook data sensitivity issues • Overlook the need for user authentication • Create systems without human design
2. Apply straightforward clinical standards	• Provide guidelines to using the system and safeguard timely assistance • Implement authentication procedures • Make procedures swift for all users • See the phone as a means, not as a medical device or a substitute to face-to-face consultation	• Create guidelines with no means of delivery • Enforce malicious compliance • Introduce contradictory clinical guidelines
3. Integrate into existing healthcare system	• Explain why a phone is being used in the consultation • Develop context-appropriate rules for phone use • Authenticate the lines of communication, to ensure the correct clinician and patient • Record key points of the digital conversation in patient notes • Seek buy-in at all levels	• Implement systems that distract clinicians from patient care in excess of existing work processes
4. Seek guidance from existing regulatory frameworks	• Develop more pragmatic guidelines at regulatory bodies • Develop discipline-specific professional society guidelines • Follow phone stewardship guidelines • Ensure that solutions' data management procedures comply with data security standards	
5. Build in protective solutions	• Follow software engineering best practice • Have adequate 'human' support structures in place • Ensure that adequate, structured data are collected via customised fields • Build in interactivity, to ensure that remote clinicians can request additional information to guide decision-making • Incorporate back-up mechanisms in the event of failure • Integrate escalation processes in the event of clinical disagreements • Provide for seamless integration into the patient's journey through the healthcare system	• Treat a product as a project • Let data go to waste • Save photos and data on clinicians' personal devices
6. Make ethics a quality assurance measure	• Align the choice and flow of data to patient safety requirements • Introduce means of rapidly detecting data breaches • Allow regular review of data quality • Provide medicolegal support to users as needed	• Assume that others know, and so refrain from regularly sharing expertise • Exclude patients
7. Focus on self-determination and governance	• Create products that support existing clinical governance strategies • Ensure adequate record-keeping of all digital interactions • Save data on cloud services	• Exclude patients from decision-making

The pillars forming the basis for the workshop discussion broadly endorsed what other publications have recommended when developing, introducing and implementing mHealth technologies.[7,11,15,16] These pillars touched upon critical ethical issues in the SA context, such as 'What security standards and procedures should apply to mobile devices used by healthcare workers?' or 'Can informed consent be collected remotely from clients using mobile devices or applications?'[14]

There are multiple examples of SA legislation that apply to mHealth projects and applications that handle client information,

such as the Protection of Personal Information Act No. 4 of 2013, the National Health Act No. 61 of 2003, and the amendments from 2014 that incorporate requirements from the National Health Normative Standards Framework for Interoperability in eHealth. The dos and don'ts presented here need to be aligned to these key legislations and, conversely, new legislation needs to take cognisance of these perspectives.

Declaration. None.

Acknowledgements. We wish to acknowledge other members of the workshop for their extensive contributions, namely Siraaj Adams, Peter Barron, Peter Benjamin, Brian DeRenzi, Katusha de Villiers, Amnesty Lefevre, Nozizwe Makola, Jessica Manim, William Mapham, Zandile Mchiza and Raveen Naidoo.

Author contributions. LAW and LL had the original idea for the workshop; LAW, LL and JC structured the workshop and led it on the day; LL drafted the article; and all authors contributed to the final article. LAW is the guarantor.

Funding. None.

Conflicts of interest. None.

1. Barit A. The apps are coming! But will they be legal in South Africa? S Afr Med J 2019;109(3):150-151. https://doi.org/10.7196/SAMJ.2019.v109i3.13812
2. Howitt P, Darzi A, Yang GZ, et al. Technologies for global health. Lancet 2012;380(9840):507-535. https://doi.org/10.1016/S0140-6736(12)61127-1
3. Saarni SI, Hofmann B, Lampe K, et al. Ethical analysis to improve decision-making on health technologies. Bull World Health Organ 2008;86(8):617-623. https://doi.org/10.2471/BLT.08.051078
4. Mytton OT, Velazquez A, Banken R, et al. Introducing new technology safely. Qual Saf Health Care 2010;19(Suppl 2):i9-i14. https://doi.org/10.1136/qshc.2009.038554
5. Korhonen E-S, Nordman T, Eriksson K. Technology and its ethics in nursing and caring journals. Nurs Ethics 2015;22(5):561-576. https://doi.org/10.1177/0969733014549881
6. Martínez-Pérez B, de la Torre-Díez I, López-Coronado M. Privacy and security in mobile health apps: A review and recommendations. J Med Syst 2014;39(1):181. https://doi.org/10.1007/s10916-014-0181-3
7. Sharp M, O'Sullivan D. Mobile medical apps and mHealth devices: A framework to build medical apps and mHealth devices in an ethical manner to promote safer use – a literature review. Stud Health Technol Inform 2017;235:363-367. https://doi.org/10.3233/978-1-61499-753-5-363
8. Laflamme L, Chipps J, Fangerau H, et al. Targeting ethical considerations tied to image-based mobile health diagnostic support specific to clinicians in low-resource settings: The Brocher Proposition. Glob Health Action 2019;12(1):1666695. https://doi.org/10.1080/16549716.2019.1666695
9. Laflamme L, Wallis L. Seven pillars for ethics in digital diagnostic assistance among clinicians: Take homes from a multi-stakeholder and multi-country workshop. J Glob Health 2020;10(1):010326. https://doi.org/10.7189/jogh.10.010326
10. Ash JS, Berg M, Coiera E. Some unintended consequences of information technology in health care: The nature of patient care information system-related errors. J Am Med Inform Assoc 2004;11(2):104-112. https://doi.org/10.1197/jamia.M1471
11. Ettinger K, Pharaoh H, Buckman RY, Conradie H, Karlen W. Building quality mHealth for low resource settings. J Med Eng Technol 2016;40(7-8):431-443. https://doi.org/10.1080/03091902.2016.1213906
12. Papadopoulos H, Pappa D, Gortzis L. A framework for dealing with legal and clinical risks arising from the use of m-Health systems. J Inf Technol Healthc 2007;5(3):182-195. https://doi.org/10.2196/jmir.3133
13. Morera EP, de la Torre Díez I, Garcia-Zapirain B, López-Coronado M, Arambarri J. Security recommendations for mHealth apps: Elaboration of a developer's guide. J Med Syst 2016;40(6):152. https://doi.org/10.1007/s10916-016-0513-6
14. Measure Evaluation. Regulating mHealth in South Africa. 2016. https://www.measureevaluation.org/resources/publications/fs-16-200 (accessed 8 September 2020).
15. Albrecht U-V, Fangerau H. Do ethics need to be adapted to mHealth? Stud Health Technol Inform 2015;213:219-222.
16. Carter A, Liddle J, Hall W, Chenery H. Mobile phones in research and treatment: Ethical guidelines and future directions. JMIR Mhealth Uhealth 2015;3(4):e95. https://doi.org/10.2196/mhealth.4538

Accepted 4 November 2020.