SOUTH AFRICAN MEDICAL ASSOCIATION

Statement on Digital Health

PREAMBLE

Digital health is a broad umbrella term that refers to "the use of information and communication technologies in medicine and other health professions to manage illnesses and health risks and to promote wellness."[1] This definition also includes telehealth, telemedicine, electronic health records (EHRs) and mobile health (mHealth).

The principles of medical ethics that are mandatory for the profession must be respected in the practice of all types of digital health.

Technological developments and the increasing availability and affordability of mobile technological devices have led to an exponential increase in the number and variety of digital health services in use in all sectors of healthcare. Simultaneously, this relatively new and rapidly evolving area remains mostly unregulated, which could have potential patient safety and ethical implications.

General Principles

The development and application of digital health has expanded the traditional channels of health care delivery, allowing access to more healthcare providers, and increasing accessibility of health care in general. At the same time, its effect on the patient-doctor relationship, accountability, multi-stakeholder interactions, and traditional ethical principles should be taken into consideration.

Digital health should not be introduced solely to cut costs or as a perverse incentive to over-service and to increase doctors' earnings.

Doctor autonomy

Acceptable boundaries in the patient-doctor relationship, necessary for the provision of optimal care, should exist in digital as well as physical practice. Digital health can potentially infringe on a doctor's personal life and privacy due to theoretical 24/7 virtual availability. The doctor needs to inform patients about availability and recommend services when he or she is not available.

Doctors should exercise their professional autonomy in deciding whether a digital health consultation versus a face-to-face consultation is appropriate. This autonomy should consider the type of visit scheduled, the doctor's comfort with the medium, and the doctor's assessment of the patient's comfort level with this type of care.

Patient-doctor relationship

[1] StatPearls - https://www.ncbi.nlm.nih.gov/books/NBK470260/

While the practice of digital health challenges the conventional perception of the patient-doctor relationship, there is a “duty of care” established in all digital health encounters between the doctor and the patient, as in any healthcare encounter.

Ideally, the patient-doctor relationship should be based on a personal examination and sufficient knowledge of the patient’s medical history. Digital health should be employed primarily when a doctor cannot be physically present within a safe and acceptable period. It could also be used to manage chronic conditions or follow-up after initial treatment, where it has been proven to be safe and effective.

The doctor providing digital health services should be familiar with the technology and/or should receive sufficient training and orientation in digital communication, including an operating toolkit that provides the clinician with teaching tools and helps change healthcare provider behaviour and practice. Additionally, the doctor should take steps to ensure that quality of communication during a telehealth an eHealth encounter is maximized, by assigning, where appropriate, specific training personnel or technicians to aid patients in the technology employed. Any significant technical deficiencies should be noted in the documentation of the consultation and reported, if applicable

The patient-doctor relationship is based on mutual trust and respect. Therefore, the doctor and the patient must identify each other reliably when digital health is employed.

In consultation between two or more professionals within or between different jurisdictions, the primary doctor remains responsible for the patient’s care and coordination with the distant medical team. Doctor supervision regarding protocols, conferencing, and medical record, including electronic health records review is required in all settings and circumstances. Doctors providing consultation should be able to contact other health professionals and technicians, as well as patients, in a timely manner.

The doctor should give clear and explicit direction to the patient during the digital health encounter regarding who has ongoing responsibility for any required follow-up and ongoing health care.

Informed consent

All relevant legislation and regulations relating to patient decision-making and informed consent also apply in digital consultations.

Proper informed consent requires that all necessary information regarding the distinctive features of digital health, in general, and telehealth, in particular, be explained fully to patients including, but not limited to: explaining how telehealth works, how to schedule appointments, privacy concerns, the possibility of technological failure, including confidentiality breaches; possible secondary use of data; protocols for contact during virtual visits, prescribing policies and coordinating care with other health professionals. This information should be provided clearly and understandably without influencing the patient’s voluntary choices.

Quality of Care

The doctor and the patient must be satisfied that the standard of care delivered via digital health is “reasonable” and at least equivalent to any other type of care given to the patient, considering the specific context, location and timing, and relative availability of regular care. If the “reasonable” standard cannot be satisfied via digital technology, the doctor should inform the patient and suggest an alternative healthcare delivery.

The doctor should use existing clinical practice guidelines, whenever possible; to guide the delivery of care in the digital setting, recognizing that certain modifications may need to be made to accommodate specific circumstances. Changes to clinical practice guidelines for the digital setting should be approved by the discipline’s clinical governing and/or regulatory body or association.

The doctor providing digital services should follow all regulatory requirements and relevant protocols and procedures related to informed consent (verbal, written, and recorded); privacy and confidentiality; documentation; ownership of patient records; and appropriate video/telephone behaviours.

The doctor consulted through digital health should keep a detailed record of the advice delivered, and the information received, and on which the recommendation was based.

The doctor should be aware of and respect the particular challenges and uncertainties that may arise when in contact with the patient through digital telecommunication. A doctor must be prepared to recommend direct patient-doctor contact whenever possible if he/she believes it is in the patient's best interests or will improve compliance.

The possibilities and weaknesses of digital health in emergencies must be duly identified. If it is necessary to use telemedicine in an emergency, the advice and treatment suggestions are influenced by the severity of the patient's medical condition and the patient's technological and health literacy. Entities that deliver telemedicine services must establish protocols for referrals for emergency services.

Clinical Outcomes

The provision of digital health programmes should monitor and continuously strive to improve the quality of services to achieve the best possible outcomes.

The provision of digital health programmes should have a systematic method of collecting, evaluating, and reporting meaningful health care outcome, safety data and clinical effectiveness. Quality indicators should be identified and utilized. Like all health care interventions, digital health technology must be tested for its effectiveness, efficiency, safety, feasibility, and cost-effectiveness.

The implementation of digital health should strive to report unintended consequences to help improve safety and further the overall development of the field. Countries are encouraged to implement these guiding principles in their own legislation.

Equity of care

Although digital health can in some ways provide greater access to distant and underserved populations, it may also exacerbate existing inequalities due to, among other things, age, race, socioeconomic status, cultural factors, or literacy issues. Doctors must be aware that certain digital technologies might be unavailable or unaffordable to patients, impeding access and further widening the health outcomes gap between the poor and the rich.

The monitoring and evaluation of digital technologies should be implemented carefully to avoid inequity of access to these technologies. Where appropriate, social or healthcare services should facilitate access to technologies as part of basic benefit packages while taking all necessary precautions to guarantee data security and privacy. Access to vital technologies should not be denied to anyone based on financial status or a lack of technical expertise.

Confidentiality and data security

The doctor must ensure that patient privacy, data confidentiality, and integrity are not compromised. Data obtained during a digital consultation must be secured to avoid unauthorized access and breaches of identifiable patient information through appropriate and up-to-date security and privacy measures per local legislation. Electronic transmission of information (electronic health records) must also be safeguarded against unauthorized access. If data breaches do occur, the patient must be notified immediately.

Digital health technologies generally involve the measurement or manual input of medical, physiological, lifestyle, activity, and environmental data to fulfil their primary purpose. The large amount of data generated also offers enormous research scope into effective healthcare delivery and disease prevention. However, this secondary use of personal data also has great potential for misuse and abuse.

Robust policies and safeguards to regulate and secure the collection, storage, protection, and processing of digital health users' data, especially personal health data, must be implemented. Users of digital health services must be informed about how their data is collected, stored, protected, and processed. Their consent or appropriate lawful justification must be obtained before disclosing personal health data to third parties, e.g., researchers, governments, or insurance companies.

Provisions must be made to allow patients: access to their personal health records; requested amendment of errors found in the records; disclosure of how their health information has been used, including persons and organizations to whom/which it has been disclosed; requests to restrict access to and/or additional protections for, confidential communications, particularly of sensitive data; limits on additional uses (such as fundraising, marketing, research) unless authorized by the patient.

If patients believe that their privacy rights have been violated, they may file a complaint with the covered entity's Privacy Officer or data protection authorities, as per local regulations.

Legal principles

Digital health should be appropriately adapted to local, national and international regulatory frameworks, including licensing digital platforms in patients' best interest.

Doctors should only practice digital according to relevant legislation and regulations. This includes, but is not limited to the Constitution of South Africa; National Health Act [No. 61 of 2003]; Health Professions Act [No. 56 of 1974]; Protection Of Personal Information Act [No. 4 of 2013], Electronic Communication Transaction Act [No. 25 of 2002], Promotion of Access to Information [No. 2 of 2000], any other applicable acts, the common law and the relevant HPCSA ethical guidelines.

Doctors should also ensure that their medical indemnity includes telemedicine and digital health coverage.

Suitable reimbursement models must be set up in consultation with healthcare providers to ensure that doctors receive appropriate reimbursement for their involvement in digital health activities.

Electronic Health Records, including the ownership thereof

EHRs is defined as the "Longitudinal collection of personal health information of a single individual, entered or accepted by health care providers and stored electronically" and where "Access to the record must be authorized by the provider and patient."" [2]

Please refer to page 5 of this document for further resources on EHRs.

Specific principles of digital health technology

A clear distinction must be made between digital health technologies used for lifestyle purposes and those that require doctors' medical expertise and meet the definition of medical devices. The latter must be appropriately regulated, and users must verify the source of information provided. The information provided must be comprehensive, clear, reliable, non-technical, and comprehensible to laypeople.

Concerted work must improve the interoperability, reliability, functionality, and safety of digital health technologies, e.g., through the development of standards and certification schemes.

Comprehensive and independent evaluations must be carried out regularly by competent authorities with appropriate medical expertise to assess the functionality, limitations, data integrity, security, and privacy of mHealth technologies. This information must be made publicly available.

Digital health can only positively contribute to improvements in care if services are based on sound medical rationale. As evidence of clinical usefulness is developed, findings should be published in peer-reviewed journals and be reproducible.

It is vital to contemplate the risks of excessive or inappropriate use of digital health technologies and the potential psychological impact on patients. The risks and benefits of the technology should be continually monitored, making sure the benefits outweigh the risks.

RECOMMENDATIONS

[2] Brivik T. 2015. Who owns your Health Records in South Africa? *Malcolm Lyons and Brivik Inc. Attorneys South Africa.* Available: https://www.hcsmsa.co.za/healthdatalaw/

Digital health has the potential to supplement traditional ways of managing health and delivering healthcare. While digital healthcare may offer advantages to patients otherwise unable to access medical services, it is not universally appropriate, nor is it always an ideal form of diagnosis and treatment.

The driving force behind digital health should be eliminating deficiencies in care provision or improving care quality and / or access.

SAMA urges patients and doctors to be discerning in their use of digital health and to be mindful of potential risks and implications.

SAMA recommends special attention to patients' disabilities (audio-visual or physical) and patients who are minors, when using digital healthcare.

SAMA recommends that regulatory bodies, professional societies, organizations, institutions, departments and regional management, monitor the proper use of digital health technologies.

****

This statement is adapted from the WMA Statement on the Ethics of Telemedicine and the Statement on Mobile Health.

The SAMA statement on Digital Health is a living document and will be continually edited and updated.

Further resources on EHRs

1. HPCSA. 2020. Guidance on the application of telemedicine guidelines during the COVID19 pandemic. https://www.hpcsa.co.za/Uploads/Events/Announcements/APPLICATION_OF_TELEMEDICINE_GUIDELINES.pdf
2. Katurura MC, Cilliers L. Electronic health record system in the public health care sector of South Africa: A systematic literature review. African journal of primary health care & family medicine. 2018;10(1):1-8. http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S2071-29362018000100081
3. Health Professional Council of South Africa. Guidelines on the keeping of patient records. https://ethiqal.co.za/wp-content/uploads/2019/08/HPCSA-Guidelines-on-the-Keeping-of-Patient-Records.pdf
4. Medical Records in South Africa: An MPS Guide. https://www.medicalprotection.org/docs/default-source/pdfs/Booklet-PDFs/sa-booklets/medical-records-in-south-africa---an-mps-guide.pdf
5. Brivik T. 2015. Who owns your Health Records in South Africa? *Malcolm Lyons and Brivik Inc. Attorneys South Africa.* Available: https://www.hcsmsa.co.za/healthdatalaw/ OR https://www.lyonsbriviklaw.com/who-owns-patient-records-in-south-africa/
6. Massaingaie W. 2021. Electronic signatures and issuing of prescriptions. SAMA Insider. http://www.samainsider.org.za/index.php/SAMAInsider/article/viewFile/116/89