WMA STATEMENT ON DIGITAL HEALTH

Adopted by the 60th WMA General Assembly, New Delhi, India, October 2009
and revised by the 73rd WMA General Assembly, Berlin, Germany, October 2022

PREAMBLE

1. Digital health is a broad 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." Digital health encompasses electronic health (eHealth) and developing areas such as the use of advanced computer sciences (including 'big data', bioinformatics and artificial intelligence). The term also includes telehealth, telemedicine, and mobile health (mHealth).

2. The term "digital health" may be used interchangeably with "eHealth." These terms also include within them: Telehealth" or "Telemedicine," which both utilize information and communications technology to deliver healthcare services and information at a distance (large or small). They are used for remote clinical services, including real-time patient monitoring such as in critical care settings. Also, they serve for patient-physician consultation where access is limited due to physicians'/patients' schedules or preferences, or patient limitations such as physical disability. Alternatively, they can be used for consultation between two or more physicians. The difference between the two terms is that "Telehealth" refers also to remote clinical and non-clinical services: preventive health support, research, training, and continuing medical education for health professionals.

3. Technological developments and the increasing availability and affordability of mobile devices have led to an exponential increase in the number and variety of digital health services in use in both developed and developing countries. Simultaneously, this relatively new and rapidly evolving sector remains largely unregulated, which could have potential patient safety and ethical implications.

4. The driving force behind digital health should be improving quality of care, patient safety and equity of access to services otherwise unavailable.

5. Digital health differs from conventional health care in the medium used, its accessibility, and its effect on the patient-physician relationship, as well as on the traditional principles of patient care.

6. The development and application of digital health has expanded access to health care and health education in both regular and emergency situations. At the same time, its effect on the patient-physician relationship, accountability, patient safety, multistakeholder interactions, privacy and data confidentiality, fair access, and other social and ethical principles should be taken into consideration. However, the scope and application of digital health, telemedicine or telehealth are context-dependent. Factors such as human resources for health, size of service area and level of healthcare facilities should also be taken into consideration.

7. Physicians should be involved in the development and implementation of digital health solutions to be used in health care, in order to ensure they meet the needs of patients and health professionals.

8. Consistent with the mandate of the WMA, this statement is addressed primarily to physicians and their role in the health care setting. The WMA encourages others who are involved in healthcare to develop and adhere to similar principles, as appropriate to their role in the healthcare system.

Physician autonomy

9. Acceptable boundaries in the patient-physician relationship necessary for the provision of optimal care, should exist in digital as well as physical practice. The nearly continuous availability of digital health care has the potential to unduly interfere with a physician's work-life balance due to theoretical 24/7 availability. The physician should inform patients about his or her availability and recommend services when he or she is not available.

10. Physicians should exercise their professional autonomy in deciding whether digital health consultation is

appropriate. This autonomy should consider the type of visit scheduled, the physician's comfort with the medium, and the physician's assessment, together with the patient, of the patient's comfort level with this type of care.

Patient-physician relationship

11. Face to face consultation should be the gold standard where a physical examination is required to establish a diagnosis, or where there is a wish on the part of the physician or patient to communicate in person as part of establishing a trusted physician-patient relationship. Face to face consultations may be preferable in some circumstances to take stock of non-verbal cues, and for consultations where there may be communication barriers or discussion of sensitive matters. Ideally, the patient-physician relationship in the context of digital health, should be based on a previously established relationship and sufficient knowledge of the patient's medical history.

12. However, in emergency and critical situations, or in settings where access to doctors is not available other than via telemedicine, delivery of care via telemedicine should be prioritized even when a prior patient-physician relationship was not established. Telemedicine can be employed when a physician cannot be physically present within a safe and acceptable period. It can also be used to manage patients remotely including self-management and for chronic conditions or follow-up after initial treatment, where it has been proven to be safe and effective.

13. The physician providing telemedicine services should be familiar with the technology and/or should receive sufficient resources, training and orientation in effective digital communication. Additionally, the physician should strive to ensure that quality of communication during a digital health encounter is maximized. It is also important that the patient is comfortable using the technology employed. Any significant technical deficiencies should be noted in the documentation of the consultation and reported, if applicable.

14. The patient-physician relationship is based on mutual trust and respect. Therefore, the physician and the patient must identify each other reliably when telemedicine is employed. However, it must be recognized that sometimes third parties or 'surrogates' such as a family member should become involved in the case of minors, the frail, the elderly, or in an emergency situation.

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

16. In a digital consultation between two or more professionals, the primary physician remains responsible for the patient's care and coordination. The primary physician remains responsible for protocols, conferencing, and medical record review in all settings and circumstances. Physicians providing consultation should be able to contact other health professionals and technicians, as well as patients, in a timely manner.

Informed consent

17. Proper informed consent requires that the patient be informed of, have capacity for, and provide consent specific to the type of digital health being used. All necessary information regarding the distinctive features of digital health, in general, and telemedicine, in particular, must be explained fully to patients including, but not limited to: how telemedicine 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 coercion or undue influence of the patient's voluntary choices, while taking into account the patient's perceived level of health literacy and other resource limitations specific to the type of digital health being used.

Quality of care

18. The physician must ensure the standard of care delivered via digital health is at least equivalent to any other type of care given to the patient, considering the specific context, location and timing, and relative availability of face to face care. If the standard of care cannot be satisfied via digital technology, the physician should inform the patient and suggest an alternative form of healthcare delivery.

19. The physician should have clear and transparent protocols for delivering digital health care such as 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 appropriate governing and/or regulatory body or association. If the digital health solution is equipped with automated clinical practice support, this support must be strictly professionally based and not influenced by economic interests in any way.

20. The physician 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 behaviors.

21. The physician providing care by means of telehealth should keep a clear and detailed record of the advice delivered, the information on which the advice was based and the patient's informed consent.

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

23. 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 will be influenced by the severity of the patient's medical condition and the patient's technological and health literacy. To ensure patient safety, entities that deliver telemedicine services should establish protocols for referrals in emergency situations.

Clinical Outcomes

24. Entities providing digital health programs should monitor and continuously strive to improve the quality of services to achieve the best possible outcomes.

25. Entities providing digital health programs should have a systematic protocol for collecting, evaluating, monitoring and reporting meaningful health care outcomes, safety data and clinical effectiveness. Quality indicators should be identified and utilized. Like all health care interventions, digital technology must be tested for its effectiveness, efficiency, safety, feasibility, and cost-effectiveness. Quality assurance and improvement data should be shared to improve its equitable use.

26. Entities implementing digital health are urged to report unintended consequences to help improve patient safety and further the overall development of the field. Countries are encouraged to implement these guiding principles in their own legislation and regulation.

Equity of care

27. Although digital health can 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. Physicians must be aware that certain digital technologies might be unavailable or unaffordable to patients, impeding access and further widening the health outcomes gaps.

28. Digital technologies should be implemented and monitored 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

29. In order to ensure data confidentiality, officially recognized data protection measures must be used. 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. If data breaches do occur, the patient must be notified immediately in accordance with the law.

30. Digital health technologies generally involve the measurement or manual input of medical, physiological, lifestyle, activity, and environmental data to fulfill their primary purpose. The large amount of data generated also may be used for research or other purposes to improve healthcare and disease prevention. However, secondary uses of personal mHealth data can result in misuse and abuse.

31. 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 to assure valid informed consent and guarantee patients' rights.

32. 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, in accordance with local regulations.

Legal principles

33. A clear legal framework must be drawn up to address potential liability arising from the use of digital technologies. Physicians should only practice telemedicine in countries/jurisdictions where they are licensed to practice and should adhere to the legal framework and regulations as defined by the country/jurisdiction where the physician originates care and the countries in which they practice. Physicians should ensure that their medical indemnity includes telemedicine and digital health coverage.

34. Reimbursement models must be set up in consultation with national medical associations and healthcare providers to ensure that physicians receive appropriate reimbursement for providing digital health services.

Specific principles of mHealth technology

35. Mobile health (mHealth) is a form of electronic health (eHealth) for which there is no fixed definition. It has been described as medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other devices intended to be used in connection with mobile devices. It includes voice and short messaging services (SMS), applications (apps), and the use of the global positioning system (GPS).

36. A clear distinction must be made between mHealth technologies used for lifestyle purposes and those that require physicians' medical expertise and meet the definition of medical devices. The latter must be appropriately regulated, and users must be able to verify the source of medical information provided, as these applications could potentially recommend non-scientific or non-evidence-based treatments. The information provided must be comprehensive, clear, reliable, non-technical, and easily understood by laypeople.

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

38. 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.

39. mHealth 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.

RECOMMENDATIONS

1. The WMA recognizes the value of digital health to supplement traditional ways of managing health and delivering healthcare. The driving force behind digital health should be improving quality of care and equity of access to services otherwise unavailable.

2. The WMA emphasizes that the principles of medical ethics, as outlined in The Declaration of Geneva: The Physician's Pledge and the International Code of Medical Ethics, must be respected in the practice of all forms of digital health.

3. The WMA recommends that the training of digital health literacy and skills be included in medical education and continuing professional development.

4. The WMA urges patients and physicians to be discerning in their use of digital health and to be mindful of potential risks and implications.

5. The WMA recommends further research in digital health to assess safety, efficacy, cost-effectiveness, feasibility of implementation, and patient outcomes.

6. The WMA recommends monitoring the risks of excessive or inappropriate use of digital health technologies and the potential psychological impact on patients and ensuring that the benefits of such technologies outweigh the risks.

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

8. Where appropriate, National Medical Associations should encourage the development and update of ethical norms, practice guidelines, national legislation, and international agreements on digital health.

9. The WMA recommends that other regulatory bodies, professional societies, organizations, institutions, and private industry, monitor the proper use of digital health technologies and share these findings widely.