CSIT (April 2023) 11(1):97–102
https://doi.org/10.1007/s40012-023-00370-5

ORIGINAL RESEARCH

Digital health rules and regulations: an overview

Bagmisikha Puhan[1] · Siddhant Gupta[1]

Received: 12 January 2023 / Accepted: 1 March 2023 / Published online: 16 March 2023

Abstract With the proliferation of digital health around the globe, there is involvement of one too many stakeholders, across the entire spectrum of service offerings. What may have started as a focus on the platforms, and care providers, now witnesses and ascribes several duties and obligations which are carved out for the end users, the patients in this case. In this article, we are deep diving into the rules and regulations involving the digital health ecosystem. Some are common across the globe, while some are still finding its bearings in a nascent community and heterogenous structure, like the healthcare system in India. This article will also highlight ethical concerns tied to the practice, especially where reliance is placed on human-centric data, submitted by individuals (caregivers, patients, alike), and populated in the devices used by the stakeholders. With challenges around privacy growing, digital health is also bracing its shields, without losing sight of the primary objective of universal health coverage and wellness being brought to the last mile.

Keywords Digital health · Law · Ethics · Medicine · Information technology · Privacy

1 Background

According to the US Food and Drugs Administration (**US FDA**), the broad scope of digital health includes categories such as mobile health (mHealth), health information [communication] technology (**ICT**), wearable devices, telehealth and telemedicine, and personalized medicine [1]. It is noteworthy that all these categories which find a mention within this definition, are heavily reliant on *human health data, inputs which are made by humans in their interactions with technology, and, ICT systems.* Against this backdrop, everyone using ICT to either seek, deliver, or enable healthcare, is bound to be aware of the benefits, as well as of any adverse consequences which may stem from their participation in this ecosystem. To this end, we shall first seek to explore the scope and limitations of digital health and examine it against the existing law and ethics framework, before we proceed to suggest the way forward. In doing so, we will also evaluate the privacy concerns and practices which exist and that which must be implemented for effective realization of the digital health goals.

2 Introduction

The discussion around digital health may have begun with focus being placed on the use of technology, however, we now see a gradual transition to reliance being placed on *data* [2]. Tied to this evaluation is the realization that there is a real transition taking place from the erstwhile *focus on cure/illness,* to wellness. This requires evaluation, analysis of copious volumes of health data, genetic and genomic data, lifestyle information—which goes beyond the individual who is the immediate concern, but brings into the fold, the entire family, genealogy, to achieve better outcomes. Interestingly, the common thread here is the data, which is being constantly fed, by the healthcare practitioner, the patient, the technology platform—and more importantly the device, which is working round the clock, unobtrusively [3].

It is better to understand certain aspects and the challenges associated with them, at this very stage. While

✉ Bagmisikha Puhan
bagmisikha.puhan@gmail.com

[1] TMT Law Practice, New Delhi, India

discussions around adoption of precision medicine, and S*oftware-as Medical-Device* are on, we are also at the cusp of *growing acceptance amongst the users.* Some say that the higher use of wearable devices may cut costs of emergency healthcare, but is that wrong? For individuals who do not have robust insurance plans, or, individuals residing in countries with fledgling healthcare infrastructure, increase in uptake of such wellness devices and protocols, will only be a step in the right direction.

2.1 Evidence based care, novel care solutions

Data variety is a key driver for this sector; this, however, comes riddled with issues related to quality of evidence, any biases, amongst other underlying issues around data consumption. Focus on data driven healthcare solutions, diagnosis, has proliferated a novel medical model for development of personalized therapeutic strategies, keeping in view the patient's unique genomic, metabolomic, and epigenomic data. Precision medicine relies upon the individual's unique phenotypes and genotypes, to determine the appropriate course of treatment, and to deliver timely and targeted prevention measures for diseases and autoimmune disorders. To put it crudely, precision medicine is based upon the four 'P' principles—known as predictive, preventive, personalized, and participatory healthcare [4]. The pandemic has been instrumental in this change of approach to healthcare delivery, with integration of multidimensional, unstructured, and disparate data sets, being relied upon for precision care and better patient outcomes. The concept seeks to challenge a "one size fits all" approach to disease management, and treatment regimens, by identifying the characteristics which expose people to a particular disease and characterizing the primary biological pathways which cause the disorder [5]. However, this process also relies upon the data, which is fed into the ICT systems, enabling them to provide outputs for continued care measures—the article discusses concerns, and way forward for these issues which persist in the healthcare ecosystem.

The Indian healthcare industry has sought to improve access to infrastructure and tools, necessary for widespread adoption in dealing with various health issues. Collaborations with international genetic testing companies, to offer targeted therapy options using affordable genomic solutions are on the rise, providing patients with a rare opportunity to benefit from the integration of new age technologies with healthcare services. Reliance upon deep learning technologies, artificial intelligence (**AI**) and future ready digital interfaces will drive the discussion around precision healthcare in India for the future. The regulatory landscape will have to adapt, adopt, and, cater to such technologies in a future ready manner, to remove any hindrances to its wide-scale adoption.

The reliance upon health data sets for focused delivery of healthcare has also found favor amongst consumers, who are the driving force behind the steady adoption of healthcare applications. Wearable devices, for example, may provide insights into a person's daily actions, allowing them to take proactive decisions on their lifestyle. According to data from the International Data Corporation's (IDC) India Monthly Wearable Device Tracker, the Indian wearables market has grown by 141% since 2021, with 14.4-million-unit shipments recorded during this period [6].

In order to develop a consumer centric framework for the acceptance and reliance of such medical devices, regulators across jurisdictions have imposed a risk-based approach to classify medical devices and rely upon submission of detailed information on the software design, adherence to privacy principles, and evidentiary proof over the validity, efficiency of the software, for use in the device.

The US FDA and the Central Drugs Standards Control Organization (**CDSCO**) have defined medical devices on similar lines, wherein a*ny instrument, apparatus, implement, machine, contrivance, implant,* in vitro *reagent, or other similar or related article, including a component part, or accessory which is intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or intended to affect the structure or any function of the body of man or other animals, and which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of its primary intended purposes, may be termed as a medical device* [7].

Importantly, the US FDA has further sought to distinguish between general wellness devices (wearables) and medical devices, which operate with a medical purpose (diagnosis software and the likes), to ensure undue compliances, conditions are not imposed upon unsophisticated devices, which do not make claims about medical benefits such as disease prevention, treatment, mitigation, or cure.

As these technologies continue to occupy/develop an entrenched position in our everyday lives, focus must be shifted towards the legitimate processing of voluminous health data by such data collectors, and its knock-on effects upon the end users. In addition, the use of AI/machine learning (**ML**) capabilities complicates matters for patients and regulators alike, with the efficiency of such systems heavily dependent upon training data sets, which are often askewed, and not representative of the demographic health status. This purports a causality dilemma, wherein more information is required to be collected for improving the AI/ML capabilities, which must further be refined in line with the global privacy principles, intended for end user protection.

Inaccuracies in data, askewed acquisition practices (at present, most AI/ML rely upon information from Caucasian populations, which cannot be *ipso facto* applied for a different demography), affordability, and regulatory challenges must be addressed, to ensure that the seemingly harmless collection of information by wearables and devices of a similar ilk do not prejudice consumer rights in the digital space.

2.2 Challenges

Two common issues which may interfere with the widespread adoption of digital health, are: (1) Awareness and Acceptability; and (2) Lack of technical wherewithal. To deal with the first challenge, with increasing efficiency, accuracy, and uptake of digital health enablers, including wearables and other devices, it is important that the *end users,* the patients, are made aware of the medical/health conditions that can be monitored, treated and [possibly] avoided, with assimilation of such technology into their daily lives. It is, however, important also to educate them on the significance of these conditions, the possible treatment options, and the best way to access clinicians, regardless of the output of such devices [8]. Where such devices are connected to the health plan, or provide inputs to the concerned clinician, it *might* also assist the practitioner with the insight to intervene. Alongside this, the clinician, their offices, will also have to be convinced to rely on inputs which are generated by these technology enablers, and be taught how to integrate them with the clinical workflow. Awareness and acceptance have to be at the ends of the caregiver, as well as the care recipient; as reciprocal trust forms one of the foremost principles of medical ethics.

In economies like India, where the government has made stellar efforts to bring about technological revolution in the sector, on a policy front [9], and has enabled deployment of telemedicine set-ups across demographics and geographies [10, 11], challenges persist around roll-out of connected healthcare information systems, infrastructure, and basic means of interoperability. All these challenges can be overcome by way of increase in government spending, public private partnerships, and fostering further dialogues between all parties (public and private, alike) to come together and allow their systems to interact with one another. To realize the goal of universal healthcare, efforts have to be made to ensure that the *data* which forms the fabric of this entire ecosystem, continues to be protected, and untarnished. The assumption that "*too many cooks spoil the broth*" can only be defeated when laws and ethical considerations around valuing data of all the stakeholders enjoy the same level of security.

3 Law and ethics

3.1 Trust

As briefly discussed above, trust forms one of the most basic requirement and principle of medical ethics. This is reciprocal in nature, as the caregiver relies on the representations of the care recipient, the patient; and similarly, the care recipient relies solely on the prescriptions of the caregiver. Its unique nature in medicine is owed to the inherent character of information asymmetry that exists between the expert (the clinician), and the non-expert (the patient) [12]. With involvement of technology, now for the caregiver, inputs from ICT systems, would also mean that in their clinical decision-making process, a further element is also added for verification and reliance. To this end, concerted efforts have to be made and the stakeholders (including ICT systems) will have to be transparent in the processes and offerings, subscribe to accountability principles, discuss about mutual benefits derived from the collaboration, and more importantly look beyond the mere realization of a privacy compliant framework.

Involvement of automated processes would also mean that codes are fed into the ICT systems, with baseline inputs which form the very basis of their performance—this necessitates that the system owner clarifies and cross-references with the caregiver about any biases and prejudices which may seep into the primitive codes, itself. Similarly, the caregiver must communicate to the care recipient about how pre-analysis has been achieved, and what it means for the care recipient to rely on such automated tools, processing and commonly available (licensed, and non-licensed) devices.

3.2 Accountability

Earlier in cases of medico-legal matters, it was easier for the law, patients to pin the blame on the caregiver; now, accountability may also lie on the patient themselves—where they choose to feed incorrect or insufficient information. It is not for this article to make determinations with respect to what happens in such cases, and whether or not the caregiver should have made their own, independent investigations or not; we are only considering aspects which define basic parameters for ascribing accountability.

Professional accountability, as we know of it today, is bound to change with AI/ML enabled processes, being incorporated into the practice of healthcare. While there are several tools available, and they are highly efficient, premature reliance can never be placed on such tools—this was best evinced in the story of IBM Watson [13]. It was soon realized that Watson, which was to assist oncologists in cancer treatment was not able to independently extract insights from breaking news in the medical literature, and was also not able to compare a new patient with the diaspora of cancer patients who have come before to discuss hidden patterns—so are we there yet, in terms of complete reliance? No! It is keeping these shortcomings in mind, that the law has always aimed to place the burden on making final determinations on the physician themselves [14], while allowing them to rely on evaluations made by ICT systems. Where reliance on AI/ ML driven diagnosis, treatment course, surgical procedures is bound to increase, there is an inherent need to at least on an ad hoc basis, prescribe evidence-based standards for ascribing accountability [15]. This will diminish any conflicts in understanding the extent of professional accountability of the practitioner.

3.3 Data privacy and security

The holy trifecta of medical ethics would be incomplete without discussion around the core element of data, and the means and modes which go into protecting the privacy and security that must be afforded to it. With every stakeholder becoming highly aware about their own rights and duties around data privacy—it is important to ensure that: (1) transparency in practice offerings and exploitation of data is maintained; (2) explicit consent is taken from the individuals who are providing their data; (3) anonymization techniques are applied, where necessary, and aggregated data sets be used where nothing more is required; and, (4) security measures are implemented in a robust manner.

This is a problem which not just plagues the developing economies (without privacy legislations), it also concerns itself with advanced jurisdictions which have well-structured health schemes, and privacy laws. The UK Information Commissioner's office has identified that the healthcare sector accounts for most of the data incidents reported to them [16]. International policy organizations [17] have made attempts to analyze and address several data governance patterns and advise on what could be the best way of implementation of the same. National data privacy frameworks, which prescribe the very foundation on which data can be collected, processed, and be used for a wider use case, with the active consent of the end users is a "must-have", and does not form anything which can be negotiated with, or ignored. While public health is something that does not require express consent to be taken separately from the individuals, for a private consultation or a family wellness program, there is nothing which precludes the individuals from giving their express consent to buy into such a program.

The laws which discuss privacy also invariably discuss how biases and prejudices can cause irremediable harm to the individuals to whom such data pertains to, and also provide recourse in such cases. Where a cogent trust-based framework is being based upon for the purposes delivery of healthcare solutions, and care continuum, it is also important that data privacy and security measures are also baked right into the heart of the implementation programs.

4 Rules and regulations

The digital health industry is oft regulated by a myriad of overlapping regulations, concerning data privacy, telemedicine, and any laws which may speak of the necessary hardware and software specifications necessary to provide interoperability between ICT systems of different healthcare institutions. We seek to provide a brief overview of the gold standards for such regulations across the world, as well as its equivalents in the Indian regulatory environment.

1. The US Health Insurance Portability and Accountability Act, 1998 (**HIPAA**) [18] is a sectoral legislation targeted at healthcare institutions and insurance providers, and forms the golden standard for regulation of health information. HIPAA imposes restrictions upon healthcare providers from disclosing health information to unauthorized personnel and further offers guidance on the availability and processes of health insurance plans. Similarly, the European Union General Data Protection Regulation (**EU GDPR**) [19] is an all-encompassing regulation, enforceable across the European Economic Area, and lays down the rules for protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. The aforementioned legislations focus on implementing a consent-based framework for handling of sensitive health information, and ensures that data handlers (be it a healthcare provider, or a data analytics service provider) are cognizant of their responsibilities, and implement the necessary practices to protect user information, and gain user confidence in such digital health services. They also provide for the rights and duties of the provider of the information, who continue to be empowered with the rights to access their own information, rectify it, and also seek to have it moved to another service provider—which forms an essential feature for healthcare ecosystem, amongst several other rights.
2. Across the European Union (**EU**), US and India [14], the primary focus of laws related to telemedicine have been to develop and foster the caregiver—care recipient relationship from an in-person perspective, and bring about the elements of trust, vulnerability, efficiency, to the digital medium. While the EU does not provide for a nuanced framework, the reliance upon existing statutes in relation to e-commerce services, data privacy and protection, information services, ensure that the data han-

dlers must action patient requests with care, and adhere to the standards of care implicit in an in-person consult.

As there are several limitations to the extent to which digital health can support the in-person aspects of healthcare, the frameworks which exist and which are being discussed, necessarily factor in the duty of care that the caregiver owes to the care recipient, and also the prescribed standard of care, from which the caregiver must never derelict. Breaching a fiduciary duty that the caregiver owes to the care recipient shall have severe implications ranging across their professional accountability, compliances expected under ICT norms and laws, consumer protection.

4.1 Way forward

Any digital health [decision-making] framework must consider the fundamental ethical principles [20] of justice, beneficence and respect for persons. Relying on the Belmont Report [20], which was written by the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, we can interpose between creating new laws, and existing norms. These ethical principles are widely accepted and resonate amongst several other life sciences norms, including those which apply to clinical research. Regulation of digital health, should premise itself on following essentials, *namely*:

1. Informed Consent—as the delivery of healthcare services across digital health range anywhere between use of wearable devices, to diagnosis, to curating a treatment plan, the care recipients *must be:*

1.1 Informed about the nature of automation, if any being deployed for delivery of care, risks and anticipated benefits of such procedures (even if its about describing how telemedicine works), alternatives (if any), purposes;

1.1 Given the option to choose between what they must be subject to (including automated processing of their data).

It is after these necessary disclosures have been made, consent be taken, to proceed with. This involves seeking consent for *a particular procedure, including consultations,* and, also a separate consent being taken for *processing of their data.* They do not always have to be interlinked—as processing could be undertaken by a separate entity. Goes without saying, that there always is the possibility for a disconnect in what is written in such disclosure forms, and what is perceived, the intention of keeping it easily comprehensible should always be there. Also, *the caregivers, providers must not seek consent forcibly—it has to be voluntary.* Tied to the concept of trust, the data owner (patient) [21] should be able to exercise control and autonomy over their data—and should be empowered with the decision to provide their consent, or refrain from it. Simply put, where the patient wants an in-person consult, the physician cannot *impose* a telemedicine consult with them.

2. Assessment of Risks and Benefits—at the very beginning of this chapter, it was discussed how there are several stakeholders in the ecosystem: the giver (physician), the seeker /recipient (patient), the enabler (ICT platform/ system owner)—each must weigh their own risks and benefits. In doing so, the stakeholders must look beyond the psychological or physical harm that may be caused, but also factor in the legal, social and economic injuries that may stem from such an intervention. Where reliance is placed on AI/ML and such other aggregated clinical decision-making tools, enablers, there should be evidence supporting, motivating the viability of the product or the process, and also the reliability that may be placed on it. While risks have to be disclosed first to the care recipient, caregiver, there should be a clear indication that potential benefits will outweigh the risks, in a balancing act.

Tied to this objective, is the silent backdrop of ethical, legal, and social implications (ELSI) considerations which are being made by several associations comprising of natural and juristic persons [22]. These associations consider several aspects of digital health, including but not limited to, health, use of different types of ICT systems in healthcare delivery, and public health.

3. Accessibility to All—with the intent to extend universal healthcare coverage to all, inclusive growth and making digital health accessible to all, diverse demographics is essential. In a data driven digital health world, if everyone is not treated, then the datasets which will be created and will be eventually consumed by other ICT systems to assist in clinical decision-making, will also turn out to be biased and prejudiced. We have already discussed here, how certain data sets are always considering a particular race, so stunted accessibility will only mean that certain genders, races, ethnicities, and age groups will always be underrepresented. This will invariably affect the quality of the data which is derived from the datasets.
4. Data Privacy and Security—it will be an entirely futile exercise where prescriptions around how to collect, access, use, preserve, secure all the data that is collected from provisioning of digital health solutions are not made. Taking an interdisciplinary approach to understand what could be the limitations that the caregiver, care recipient, and enabler suffer from, may yield in formulation of rules and regulations which can be imple-

mented across the entire spectrum of stakeholders, and be technology as well as use-case agnostic. With several laws already in place across the globe, similar considerations and frameworks may be created and implemented across jurisdictions which lack a comprehensive framework.

The discussions referenced here consider the factual relevance of several technological advancements, and the legal and ethical challenges and requirements which must be made now. In doing so, the objective continues to be that the patient remains the focal point, data remains of paramount importance, and trust and accountability continue to form the most basic relationship that exists between the caregiver, care recipient and enabler. We have come a long way from the old adage of *health is not valued till sickness comes,* and where we are aiming to provide a closed loop of care continuum to all, we can not fall short on any of these expectations.

Declarations

Conflict of interest No financial support and no other known, or potential conflict of interest relevant to this article is to be reported.

References

1. US Food and Drug Administration. What is Digital Health? https://www.fda.gov/medical-devices/digital-health-center-excellence/what-digital-health. Last Accessed 18 Dec 2022
2. Swiss Medical Weekly. Doi: https://doi.org/10.4414/smw.2018.14571. https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/239873/Vayena_239873.pdf?sequence=2. Last Accessed 18 Dec 2022
3. Baumert M, Cowie MR et al (2022) Sleep characterization with smart wearable devices: a call for standardization and consensus recommendations. Sleep 45(12):zsac183. https://doi.org/10.1093/sleep/zsac183
4. Quazi S (2022) Artificial intelligence and machine learning in precision and genomic medicine. Med Oncol 39:120. https://doi.org/10.1007/s12032-022-01711-1;lastaccessedonDecember18,2022at1730hrs
5. Chakraborty S, Wagh A, Goel P, Phatak S (2022) Personalized medicine in India: mirage or a viable goal? Indian J Rheumatol 17:57–64. https://doi.org/10.4103/injr.injr_152_21
6. Anand S. India Wristwear Market Grows Multifold in 2021, Rising 141% YoY and Shipping 14.4 Million Units; Says IDC; International Data Corporation. https://www.idc.com/getdoc.jsp?containerId=prAP48869122. Last Accessed 19 Dec
7. United States Code, Title 21, Chapter 9, Federal Food, Drug and Cosmetics Act, Section 201(h). https://www.govinfo.gov/content/pkg/COMPS-973/pdf/COMPS-973.pdf. Last Accessed 14 Dec 2022
8. Baumert M, Cowie MR, Redline S, Mehra R, Arzt M, Pépin JL, Linz D (2022) Sleep characterization with smart wearable devices: a call for standardization and consensus recommendations. Sleep 45(12):zsac183. https://doi.org/10.1093/sleep/zsac183
9. National Health Portal, Health Policies, Ministry of Health and Family Welfare (MoHFW), Government of India. http://www.nhp.gov.in/health-policies_pg. Last Accessed 17 Dec 2022
10. Ministry of Health and Family Welfare (MoHFW), E- Health and Telemedicine. https://main.mohfw.gov.in/Organisation/departments-health-and-family-welfare/e-Health-Telemedicine. Last Accessed 17 Dec 2022
11. Ministry of Health and Family Welfare (MoHFW), National Teleconsultation Service. https://esanjeevaniopd.in/About. Last Accessed 17 Dec 2022
12. George M (2022) Trust in public health practice. Econ Polit Wkly 57(7):15
13. Strickland E (2019) IBM Watson, heal thyself: how IBM overpromised and underdelivered on AI health care. IEEE Spectr 56(4):24–31. https://doi.org/10.1109/MSPEC.2019.8678513
14. Telemedicine Practice Guidelines (2020) Appendix 5 of the Indian Medical Council (Professional Conduct, Etiquette and Ethics Regulation, 2002) Ministry of Health and Family Welfare, Government of India. https://www.mohfw.gov.in/pdf/Telemedicine.pdf. Last Accessed 19 Dec 2022
15. Elenko E, Speier A, Zohar D (2015) A regulatory framework emerges for digital medicine. Nat Biotechnol 33:697–702. https://doi.org/10.1038/nbt.3284
16. Information Commissioner’s Office. Data Security Incident Trends. https://ico.org.uk/action-weve-taken/data-security-incident-trends/. Last Accessed 20 Dec 2022
17. Organization for Economic Co-operation and Development. Recommendation of the Council on Health Data Governance. https://www.oecd.org/health/health-systems/Recommendation-of-OECD-Council-on-Health-Data-Governance-Booklet.pdf. Last Accessed 14 Dec 2022
18. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 (1996). https://www.govinfo.gov/app/details/PLAW-104publ191. Last Accessed 19 Dec 2022
19. Regulation (EU) 2016/679 of the European Parliament and of the Council Of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Last Accessed 13 Dec 2022.
20. National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. The Belmont Report Ethical Principles and Guidelines for the Protection of Human Subjects of Research. US Department of Health and Human Services. https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/read-the-belmont-report/index.html. Last Accessed 12 Dec 2022.
21. Electronic Health Record Standards for India (2016) Ministry of Health and Family Welfare. https://www.nhp.gov.in/NHPfiles/EHR-Standards-2016-MoHFW.pdf. Last Accessed 12 Dec 2022
22. Nebeker C, Torous J, Bartlett Ellis RJ (2019) Building the case for actionable ethics in digital health research supported by artificial intelligence. BMC Med 17:137. https://doi.org/10.1186/s12916-019-1377-7