International Journal of Standardization Research
Volume 18 • Issue 1 • January-June 2020

Standardizing Social Justice in Digital Health:
An HDI-Informed Health Informatics Architecture

Mamello Thinyane, United Nations University Institute in Macao, Macao

ABSTRACT

The bivalent nature of technology and its potential for adverse impacts are giving impetus to global efforts to ensure that the outcomes of technology are consistent with societal values and desired futures. Instruments such as legislation, standards, and ethical frameworks are being employed towards this end. This research investigates the domain of digital health, specifically health informatics, and asks the questions: What values should inform technical solutions in this domain? How can data justice, the infusing of social justice imperatives in data systems, be standardized in this domain? The paper presents findings from a review of data justice in health informatics supported by findings from a survey that explored key considerations for health data collection, processing, use, sharing, and exchange. The paper then presents the operationalization of the human data interaction framework through a health informatics system architecture to illustrate how the principles of legibility, agency, and negotiability can be standardized, mainstreamed, and embedded in health informatics.

KEYWORDS

Data Justice, Digital Health, Human-Data Interaction, Standardization

DOI: 10.4018/IJSR.20200101.oa2

INTRODUCTION

As Postman aptly noted, "Technology giveth and technology taketh away, and not always in equal measure. A new technology sometimes creates more than it destroys. Sometimes, it destroys more than it creates" (Postman, 2013). The benefits of technology in society have been innumerable: enhancement of trade and economy, improvements to governance, transportation, health, education, leisure and entertainment, and livelihoods. The ensuing fourth industrial revolution (4IR) and the associated frontier technologies are also set to transform society in many fundamental ways including through the societal evolution towards the infosphere (Floridi, 2014), human augmentation through biotechnology, and the pervasiveness of robotics, autonomous computing and artificial intelligence (AI).

The potential of technology to contribute to advancing sustainable development imperatives is broadly recognized hence the explicit inclusion of technology as a means of implementation for the UN Sustainable Development Goals. Notwithstanding these benefits, the challenges and risks presented by technological developments are also increasingly being recognized and understood including growing inequalities, new forms of marginalization and exclusion, algorithmic bias and injustice, digital waste, the decimation of norms, and what has broadly been termed the "dark side" of technology.

This bi-valent nature of technology and its potential to have adverse impacts in society is giving impetus to global efforts to ensure that the outcomes of technology are consistent with the societal values and desired futures. At various levels (e.g., organizational, national, global) and across many societal domains, including digital health, which is the focus of this research, there are efforts to standardize, mainstream, and embed societal goals in technology solutions. Some of the instruments that are being used towards this include legislation, standards, and ethical frameworks.

Legislation provides a legal and mandatory regulatory framework towards specific societal outcomes. While the legislative process has often been blamed for being too slow in addressing the challenges introduced by technological developments, it provides an effective mechanism for legal enforcement. Some of the relevant legislation for digital health is around the protection of individuals' privacy in data systems, for example, the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and the Protection of Personal Information Act (POPIA).

Beyond legislation, standards provide a consensus creation mechanism that provides voluntary "rules, guidelines and characteristics for activities or their results, aimed at achieving the optimum degree of order in a given context" (ISO, 2019). Although they have traditionally been technical documents and operated within the technical domain, standards have implications beyond technology and are being used to address broad societal issues such as responsible innovation, sustainability, justice, and ethics (Busch, 2011; De Vries et al., 2018; Jakobs, 2019; Wickson & Forsberg, 2015). Examples of relevant standards for the digital health domain include the ISO/

IEC 29100:2011 "Information technology, security techniques, privacy framework" standard on privacy protection of personally identifiable information (PII) (ISO/IEC, 2011) the Global Privacy Standard, as well as the work of the International Telecommunication Union (ITU) Focus Group on Data Processing and Management (FG-DPM) within Working Group 3 on "Data sharing, interoperability, and blockchain" as well as Working Group 4 on "Security, privacy and trust including Governance."

Lastly, ethical frameworks, such as Ethical OS ("Ethical OS Toolkit," 2005), Data Ethics Framework ("Data Ethics Framework," 2018), and Asilomar AI principles ("Asilomar AI Principles," 2017), are increasingly also being formulated by various stakeholders to inform technology design and use.

Fundamentally, these instruments aim to standardize, mainstream, and embed normative societal goals in technology solutions. It has been proposed that training 'good' engineers – who have not only professional virtue and character, technical excellence, but also non-technical excellences such as techno-social sensitivity, respect for nature, and commitment to the public good, could achieve the same goal of infusing technology solutions with social justice and ethical considerations (Harris, 2008). In reality, it is invariably necessary for these legislation, standards, and ethical frameworks to be operationalized to inform specific technology design processes and to be translated into specific technology requirements (Danezis et al., 2015). From a software engineering point of view, approaches such as Goal-Oriented Requirements Engineering (GORE) are an attempt at this objective of connecting technology solutions to high-level business or societal goals (Lapouchnian, 2005). Another approach, pursued in this research, is to translate these high-level ethical and social justice principles into technology design artifacts (e.g., architectural patterns, software frameworks, and design patterns) as a way to standardize them in technology solutions.

The paper is structured as follows: the next section provides an overview of digital health, focusing on health informatics and the value proposition of data for health. That is followed by a discussion of data justice and its relevance to digital health and health informatics. Various formulations of data justice are discussed, after which is distilled a list of requirements to inform technology designs. A proposal of a health informatics architecture that is informed by and that embeds the data justice principles is then presented. Lastly, the merits of this architecture are discussed, juxtaposed with other related technologies.

DIGITAL HEALTH AND HEALTH INFORMATICS

Digital health, the confluence of information and communication technologies (ICTs) and health, has opened up numerous opportunities to both enhance the delivery of existing health interventions and introduce new technology-driven health interventions (World Health Organization, 2018). Digital health includes telehealth, tele-consultants, tele-coaching, social networking, and online communities, online access to records, as well as independent self-monitoring apps. The 71st World Health Assembly recognized

the potential of technology and innovation to enhance health services. It underscored the need to "ensure that digital health solutions complement and enhance existing health service delivery models, strengthen integrated, people-centered health services and contribute to improved health, and health equity, including gender equality, and addressing the lack of evidence on the impact of digital health" (World Health Organization, 2018).

One of the core components of digital health is health informatics, comprising the technologies for the management of electronic health records, medical data, health indicators, and personal health data. Traditionally, the bulk of health data collection and processing was undertaken by health service providers, with individuals as the primary sources of health data, as well as the primary beneficiaries of the health outcomes associated with the use of the data. This data, which represents one of the critical resources for the business operation of health providers, typically exists in the form of electronic health records. However, with the growing ubiquity of health technology tools, individuals are increasingly also participating in the collection and management of their health data. In the context of personal health informatics, individuals are collecting data for self-management of their health, including to inform behavior change and track progress on specific health goals.

A survey was undertaken in this research to explore and understand individuals' use of personal health informatics. It explored individuals' motivations for data collection and monitoring, their current practice around health monitoring, as well as their attitudes and values on data sharing and social sensemaking. The survey consisted of 14 questions on demographics, personal health informatics practice, sustainable development goals, data sharing, and an open-ended question on the current practice (i.e., framed as "What information and data do you use in your everyday life that you find relevant for your wellbeing?"). The 981 respondents in the survey, the majority of whom are from North America, were recruited via virtual snowballing, social media channels, and a research panel via an online survey platform. While the participant recruitment approach and the survey platform used invariably introduced a level of bias and lack of randomness in the data sample, due to the exploratory framing of the research, the findings provided key and specific (i.e., not broadly generalizable) insights on individuals' use of personal health informatics. These findings are interspersed in and support the discussions that follow in this paper.

Personal Health Informatics

Li *et al.* (2010) formally define personal health informatics as a class of applications "that help people collect and reflect on personal information." The personal informatics field has gained increasing popularity due to several developments, including the rise of quantified-self movement (Marcengo & Rapp, 2014), the availability of affordable self-tracking technology, and the proliferating phenomenon of datafication of individuals and societies (Mai, 2016). The promise of the self-tracking devices to offer individuals a non-subjective and unambiguous assessment of their physical wellbeing and the state of their bodies has been part of society for over a century;

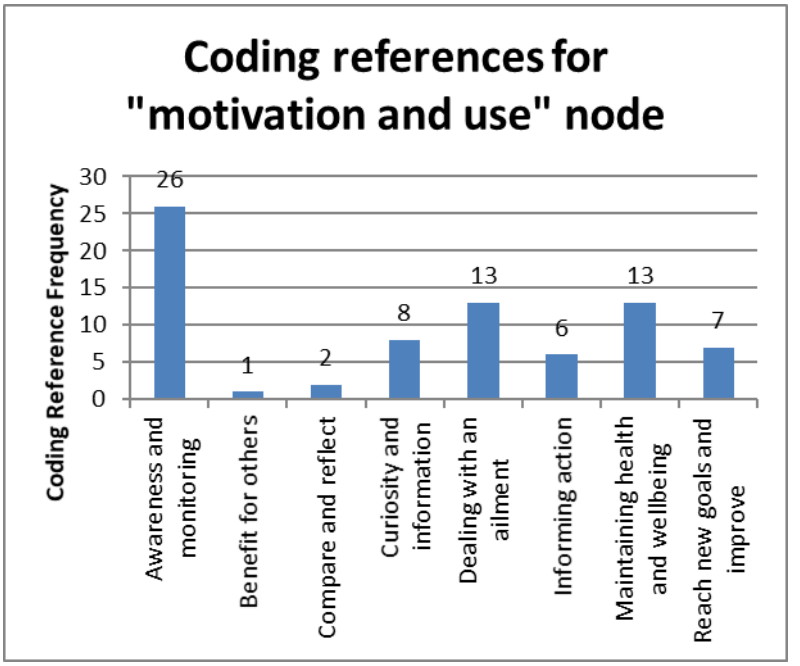
the weigh scales have played a predominant role in this regard (Crawford, Lingel, & Karppi, 2015). Beyond the development of new technologies used for personal health informatics, the 21st-century self-tracking landscape has also introduced new considerations, including the commoditization of personal data, new value dimensions associated with aggregate data, and the broad sharing of data beyond the individuals who the data is about (Boyd & Crawford, 2012; Crawford et al., 2015). Therefore, while personal informatics fundamentally regards the use of own data by individuals for their benefits, the contemporary reality is that personal data and its use exists within a broad, multifaceted ecosystem.

The use of data towards the achievement of health outcomes has traditionally been premised on the argument that more and better data leads to better health choices and decisions, and that the increasing availability of health information on the Internet would lead to the emergence of 'informed patients' (Henwood, Wyatt, Hart, & Smith, 2003) and 'digitally engaged patients' (Lupton, 2013). The transtheoretical model (TTM) of behavior change (Prochaska & Velicer, 1997), which has been the predominant model for the psychology of intentional behavior change, has also informed the formulation of personal health informatics models such as the stage-based model of personal informatics (Li et al., 2010) and the lived informatics model of personal informatics (Epstein, Ping, Fogarty, & Munson, 2015). In our research, we have identified, through the thematic coding of the open-ended survey question, the predominant pathways to impact as well as the motivations and current practice of the participants regarding personal informatics. Figure 1 highlights the primary "motivation and use" themes with their corresponding coding reference frequencies.

The motivations and uses of personal health informatics identified in our research correspond to three out of five of Rooksby *et al.* (2014) styles of personal information tracking (see Table 1). These observations support the position that as individuals engage in the collection and use of personal health data, through various impact pathways and a combination of personal conversion factors (Nambiar, 2013), they are empowered to pursue and achieved desired health outcomes. This empowerment narrative of personal health informatics has informed many digital health programs and projects around the world. It has, however, been criticized and shown to present an overly simplified techno-utopian perspective that fails to consider the nuanced complexities of personal health informatics.

Firstly, while the importance of the informational and technology resources cannot be denied, the empowerment narrative fails to recognize the difference in the agency as well as the endowment of conversion factors, such as underlying data and digital illiteracies, as well as general illiteracy, for different individuals and population groups (Nambiar, 2013). Henwood *et al.* (2003) noted these factors in an empirical research investigating "informational practices" of 32 mid-life women on the use of hormone replace therapy (HRT) for the relief of menopausal symptoms. They found that there was a strong reluctance by the participants to take on the implied responsibilities of data management; they observed problems with the information literacy of the

Figure 1. Motivation and uses of personal informatics



participants, and they also observed challenges associated with information-sharing in medical encounters with health professionals.

Secondly, the proliferation of personal health informatics technologies that track and monitor individuals' everyday functioning has the potential to unleash Orwellian techno-dystopia of panoptic surveillance assemblages that extend paternalistic social control by the strong and the powerful (D. Haggerty, Richard V. Ericson, 2000; Morley & Floridi, 2019). Beyond the risks of social control, this has the potential to open up individuals to the risks of exploitation through surveillance capitalism and commoditization of personal data, as has been demonstrated, for example, in the cases of 23andMe, Facebook, and Cambridge Analytica (Sharon, 2018; Sterckx, Cockbain, Howard, Huys, & Borry, 2013; Zuboff, 2015).

Thirdly, the empowerment narrative echoes the technological determinism sentiments, which are not universally valid and consistent. In our survey results, on the investigation of the participants' use of personal health informatics towards health outcomes and the attitudes towards data sharing, we coded 18 references that expressed both a strong resistance and refusal to use or to share personal health data. For example: "*I don't use information or data. I take my medicines and vitamins, and see my doctor often*" (GIS_806); "*How I feel, do not use data*" (GIS_504), "*Mindfulness of my moods and stress level; awareness that I am the major actor in my life, but that I can't control anything outside myself*" (GIS_379), where the participants emphasized the reliance on self-awareness as opposed to on technology devices and data; "*Actually none because*

Table 1. Motivations and styles of personal informatics

Motivation & use / Tracking style	Directive	Documentary	Diagnostic	Rewards	Fetishised
Awareness and monitoring		X			
Benefit for others					
Compare and reflect			X		
Curiosity and information					
Dealing with an ailment	X		X		
Informing action	X				
Maintaining health and wellbeing		X			
Reach new goals and improve	X				

everything changes and everyone has their viewpoint to make you believe what they are telling is true" (GIS_596), expressing the lack of trust in the system stakeholders.

Health informatics tools and technologies are employed to empower patients to achieve better health and to improve health service delivery by health service providers. The impact pathways from these digital resources to specific health outcomes are non-trivial and need to be critically understood, taking into consideration the situations of the different actants, the contextual factors, as well as the overall digital health ecosystem.

Health Data Ecosystem

Individuals are the primary subjects within the health domain, as far as being the primary beneficiaries of the targeted health outcomes. They, however, exist as one of the actants within a complex ecosystem consisting of a variety of stakeholders, including health service providers, health industry stakeholders, public sector entities, households, and communities, as well as other civil society stakeholders. The use of data towards the achievement of health outcomes, therefore, permeates this complex ecosystem and needs to be considered taking into consideration the interactions with and the data exchanges between the different stakeholders.

Firstly, in the context of the sustainable development data ecosystem or that of future data-driven societies, sharing of personal data needs to be considered not only within individuals' social circles but also with other stakeholders in the broader data ecosystem. For example, the role of citizen-generated data to support the monitoring of progress towards the sustainable development goals, through direct contributions to the indicators or via proxy indicators, has been recognized and well highlighted in the literature.

Secondly, while deriving relevant insights from health informatics ensues primarily through the individual's engagement with their data, research has found that individuals also engage in sharing of their data with others for sensemaking purposes (Fleck & Harrison, 2015; Puussaar, Clear, & Wright, 2017; Stals, Smyth, & Mival, 2017).

Thus, the collection, use, and valorization of data by individuals also comprise the social dimension.

Thirdly, personal health data also gets shared to support external pursuits such as biomedical research, where data on health profiles, cohort data, as well as physical activity data can support projects such as the Global Alliance for Genomics and Health (Knoppers & Thorogood, 2017). The sharing of data in this context can be motivated from the perspective of the Universal Declaration of Human Rights, which recognizes the "right of everyone to share in scientific advancement and its benefits" (Knoppers & Thorogood, 2017). Thus sharing of data can be towards these goals, which are associated with citizen science, as well as increased participation and engagement in advancing scientific research (Woolley et al., 2016).

In all these cases of external sharing of personal health data, there is, however, the persistent risk of "Googlization of health research," which is associated with the increasing data-driven encroachment and involvement of the major technology companies within the health and biomedical sectors (Sharon, 2018). The potential benefits of the application of these technological developments on issues of health and wellbeing are immense; they include significant improvements in disease diagnosis, improving access to services through telehealth solutions, and advancing the developmental aspirations of achieving universal health coverage. The challenges, however, are equally immense and are associated not only with adverse health outcomes but also with negative socio-cultural and economic consequences. These challenges are related to issues of bias, privacy (Jacobs & Popma, 2019), informed consent, context transgressions (Nissenbaum, 2010), health data commoditization, new power asymmetries and discriminations (Taylor, 2017), data valorization and benefit-sharing, and the importation of digital capitalism practices into the health realm (Sharon, 2018).

DATA JUSTICE IN HEALTH INFORMATICS

Numerous definitions of "data justice" have been advanced in the literature, which fundamentally recognize the social justice dynamics and impacts of data in society. Taylor (2017) defines data justice as the "fairness in the way people are made visible, represented, and treated as a result of the production of digital data." In her formulation of data justice, she decomposes the concept to three notions of *(in)visibility* – associated with *access to representation*, and *informational privacy*; *(dis)engagement with technology,* which is linked to *sharing in data benefits* as well as *autonomy in data choices*; and to *anti-discrimination,* which is linked with the *ability to challenge bias* and *preventing discrimination*. Heeks and Renken (2018) define data justice as "the primary ethical standard by which data-related resources, processes, and structures are evaluated." They, however, expand this to formulate five notions of procedural, instrumental, rights-based, structural, and distributive data justice. As noted by Taylor (2017), the end of various data justice formulations is to achieve both specific outcomes and also specific configurations of the associated data assemblages towards the achievement of those outcomes: in the case of Johnson's (2016) framework, the

end goal is embedding anti-discrimination principles and features in the design of database systems; for Heeks and Renken (2018), the focus is on data distribution in a way that achieves fair access, participation and representation; and lastly, Dencik *et al*. (2016) are interested in the means of limiting data collection and distribution in contexts of surveillance capitalism.

In the work of Mortier *et al*. (2014), in which they formalize the notion of human-data interaction (HDI), they explicate the interaction between humans and data systems in a way that places "the human at the center of the flows of data, and providing mechanisms for citizens to interact with these systems and data explicitly." While the formulation of HDI is not explicitly from a social justice nor ethics perspective, it gives recognition to the fact that the underlying issues in HDI sit at the intersection of "the various disciplines including computer science, statistics, sociology, psychology, and behavioral economics" (Mortier et al., 2014). Further, it gives recognition to the fact that human-data interaction happens in the context of complex data ecosystems, which are constitutive of the global data-driven society. In this complex interaction of different stakeholders with different capabilities, interests, and agendas, there is an ongoing contestation for the voices of humans and human-centric perspectives not to be marginalized and excluded. Some of the influential and primary actants within the health informatics ecosystem include health-service providers, the health industry, as well as the non-human technology-related actants, as has been highlighted by Sharon (2018) regarding the influence of the technology companies in the health data research. Further highlighting the complexity, Morley and Floridi (2019) offer a poignant critique of the techno-utopian formulation of mHealth technologies as empowering devices and warn against the risk of medical paternalism. Privileging the position of the humans within the health informatics ecosystem, as has been done in the HDI framework, allows for the critical investigation of issues towards an explicit goal of enhancing the substantive freedoms of individuals to achieve their desired health outcomes and enhancing their health capabilities (Ruger, 2006).

In this paper, the HDI framework has been adopted to frame the discussion of the outworking of data justice in health informatics systems. The paper expands on the imperatives of *legibility*, *agency,* and *negotiability* to identify specific considerations and non-functional requirements to inform the design of health informatics systems.

Legibility

Legibility is defined summarily as "being able to be understood by people they concern, as a precursor to exercising their agency" (Mortier et al., 2014). Legibility is defined in terms of individuals' ability to understanding what data has been collected, as well as how, when, and by whom data is being used. However, legibility is also defined with regards to the algorithms that process the data, towards ensuring that algorithms are understood and that the various forms of algorithm opacity are reasonably mitigated (Burrell, 2016). While at a simple level the "concerned" people could be understood to refer to the people who the data is about, in reality, the people who are impacted by collected health data, which Loi (2019) terms as digital phenotypes and the nature of

the impact are very diverse. In the case of health informatics, there are the identified individuals who the data is about; there are individuals who collect the data and who are involved in the creation and shaping of the digital phenotypes, and there are also people who are impacted by generalizations that emanate from health informatics (Loi, 2019). In this paper, the notion of "ownership" of data is used in the first sense, which regards health informatics as the self-extension of and as being constitutive of the individual who the data is about.

From the analysis of Mortier *et al*. 's (2014) description and discussion of "legibility," supported by the investigations undertaken in this research, the following health informatics systems requirements and considerations are formulated:

1. Accounting and auditing - to keep track of and enable an inspectable audit of the use of personal health data. Further, to allow for the auditing of the associated algorithms.
2. Feedback and notifications - to inform the owners of the collection and use of their data.
3. Relevant insights - to provide actionable insights that facilitate the subsequent use of the data.

Agency

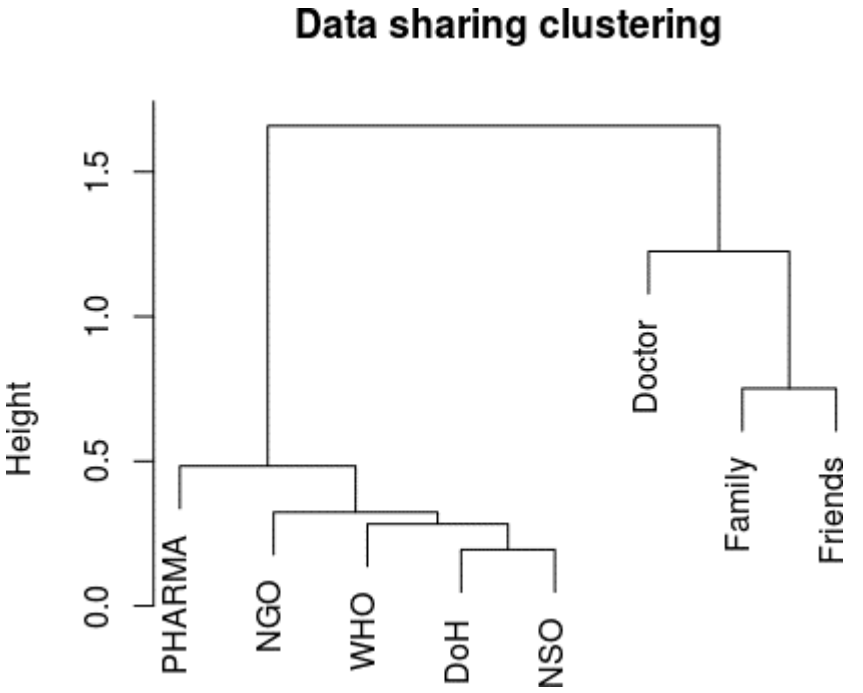
Agency is defined in terms of enhancing "the capacity for the humans to act in these data systems" (Mortier et al., 2014). Enhancing individuals' agency does not presuppose their intention to participate and to be engaged in the active management of their data, as observed in Henwood *et al*. 's (2003) research, where participants showed reluctance to take on the responsibility of managing their data. It instead has implications on the technology affordances that enhance the ability of individuals to act on and with their data meaningfully. The requirements that emanate from the undertaken analysis include:

1. Permissions and access control - the ability of individuals to permit and restrict certain types of use of their data by different stakeholders.
2. Consent and withdrawal - to enable individuals to consent to data collection and to withdraw and exercise the right to be forgotten.
3. Revocation of data - beyond the ability to withdraw from data collection, individuals should have the ability to have previously recorded data revoked and deleted.

Negotiability

Negotiability is defined in terms of "active and engaged interaction with data as contexts change." This definition makes recognition of the fact that not only do situations and contexts change, but also do individuals' desires, attitudes, and preferences. The use of personal health data is tightly coupled to and contingent on the context; individuals need to retain the legibility and agency in different contexts. The negotiability factor further decomposes into the following considerations:

Figure 2. Data-sharing stakeholder clusters



1. (Perpetual) Control - the continued ownership and control of personal health data and digital phenotypes, the digital traces that have value towards specific health outcomes, in perpetuity (Loi, 2019).
2. Data provenance - with the changing contexts and the evolution of data, it is vital to maintain the genealogy of personal health data.
3. Contextual integrity (Nissenbaum, 2010) - the significance of which is illustrated in the investigation that explored the willingness of participants to share their health data with specific stakeholders within the data ecosystem (i.e., the question was framed as "To what extent would you be happy to share your personal health information with the following individuals/organizations?"). A correlation (i.e., Spearman correlation) and clustering (i.e., agglomerative hierarchical clustering with complete linkages method using Euclidian distance between the scores) analysis of the responses indicated three distinct contexts within which the participants would share their data: with their doctors, with their families and friends, and with external organizations and stakeholders (see Figure 2). Each of these contexts represents specific requirements and preferences regarding data use.
4. Anonymization, delinking, and data commons - the ability to anonymize and delink data and to facilitate the ability of individuals to share their data broadly within the data ecosystem (e.g., to support scientific research by contributing to data commons).

Decomposing these three goals of *legibility*, *agency*, and *negotiability* into the specific requirements listed above provides an approach to connecting high-level social justice and ethics goals with technology solutions. While these requirements can be used to inform specific technology solutions, in this research, they have been embedded into a technology design artifact (i.e., software architectural pattern) as a way to generalize and standardize these goals for further derivative solutions.

HDI-INFORMED ARCHITECTURE

The architecture proposed in this paper is framed for a particular digital health scenario with specific requirements and a specific context. The scenario is that of sharing personal health informatics data (e.g., health indicators collected on personal monitoring devices, historical health records and digital phenotypes (Loi, 2019)) with a health service provider, and ensuring *legibility*, *agency,* and *negotiability* in the interaction between the individual and their data.

It is important to note that a subset of the requirements detailed in the previous section can be met and implemented with existing software engineering techniques. For example, some of the requirements around data privacy can be handled using information security techniques, such as public cryptography systems (Gardiyawasam Pussewalage & Oleshchuk, 2016), as has been the practice for, say, HIPAA compliance and, more recently, GDPR compliance. However, there are specific requirements associated with the HDI imperatives, specifically *negotiability,* that give motivation for the architecture proposed in this paper. In particular, the architecture addresses the requirement for enhancing the control that owners of data retain over their data once the data is shared and ensuring that the dynamic contextual constraints are enforced on the subsequent use of the data.

The proposed architecture, Personal Health Information eXchange (PHIX), is based on the multi-agent systems (MAS) paradigm. As a candidate implementation of this architecture, the JADE multi-agent system platform is considered (Bellifemine, Poggi, & Rimassa, 1999). JADE is a framework to develop agent applications in compliance with the Foundation for Intelligent Physical Agents (FIPA) standard for interoperable multi-agent systems. FIPA aims to provide a reference model for the implementation of highly interoperable complex agent systems. The FIPA standard defines a minimum set of essential agents that are necessary for the operation of MAS platforms. These agents include the Agent Management System (AMS) – which provides for the management and control of other agents on the platform; the Agent Communication Channel (ACC) – which provides the communication mechanism between agents on the platform; as well the Directory Facilitator (DF) which provides yellow page services for the agent platform. Besides providing the basic features that are specified in the FIPA standard, JADE provides a JAVA-based distributed agent platform, with transport mechanisms for inter-agent communication, automatic registration of agents with the AMS, a GUI for the management of the agent platform, a library of FIPA

interaction protocols, as well as functionality for monitoring the interactions between the agents (Bellifemine et al., 1999).

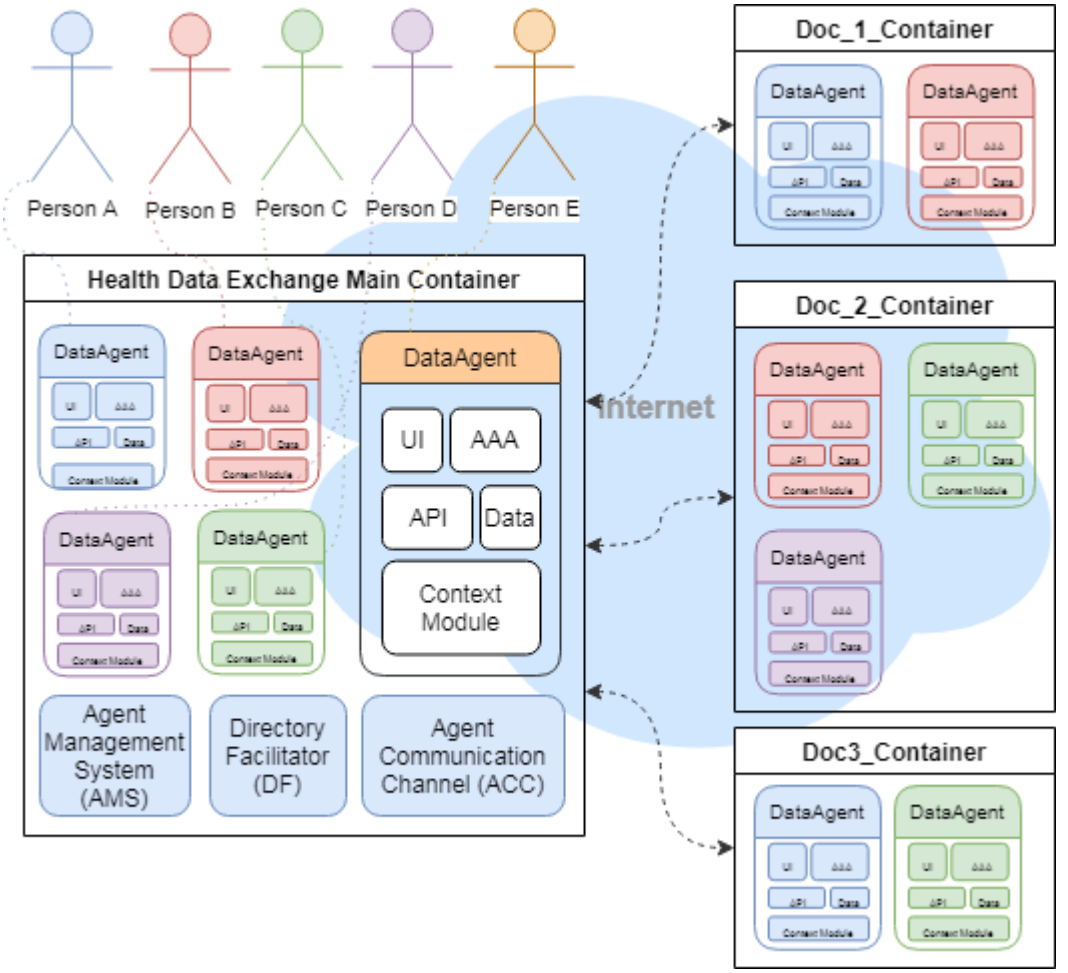
PHIX consists of the core MAS platform, distributed agent containers hosted by the health service providers, and the *DataAgent,* which encapsulates personal health data, as well as the functionality associated with the use of the data (see Figure 3). The primary element of this architecture is the *DataAgent,* which functions as a mobile virtual data double that allows for individuals' health data to be securely packaged, using relevant knowledge representation standards and ontologies (e.g., triple-based RDF or RDFS). The *DataAgent* allows for the data along with the functionality (e.g., access control, auditing, context integrity checks) to use the data to be shared with the health service providers. This data sharing is achieved through the cloning and migration of the *DataAgent* from the PHIX main container to the service provider containers. The PHIX platform also provides inter-agent communication and synchronization between the associated *DataAgents*. The data owner has control of his community of *DataAgents* with the ability to gain visibility of where his data has been shared, to understand the specific utilization of their data and to control the use of specific *DataAgents,* for example, updating permissions and access control, revoking and killing shared agents.

Within this architecture, as per the defined scenario, service discovery is primarily handled via the use of the DF through which the health service providers publish their details. Individuals who need to share their data (i.e., via cloning and migration) would similarly employ the DF to query the data for the relevant health providers. The key feature of this architecture is to bundle personal health data along with the functionality to manage its use in various contexts into the *DataAgent*, which is under the control of the data owner. By exploiting the agent mobility and migration feature of MAS, sharing of data is not associated with relinquishing control over the data, the *DataAgent* enforces the contextual constraints, as well as the dynamic access controls decided by the data owner.

DISCUSSION

Principles such as *legibility*, *agency*, and *negotiability* in data systems represent normative ethical and social justice values of society. Mainstreaming such principles in technology solutions can be achieved through legislation – towards enforceable legal stipulations, through standards – as consensual voluntary guidelines and rules, or through ethics frameworks. Another mechanism for standardizing, mainstreaming, and embedding such principles in technology solutions is by translating them into technology design artifacts, such as the PHIX architecture presented in this paper, to facilitate direct implementation. These design artifacts not only allow for direct embedding of high-level societal goals in technology solutions but as illustrated by Fernandez *et al.* (2012) they also support the operationalization of standards and their necessary translation into specific system requirements.

Figure 3. Proposed PHIX Health informatics architecture



The PHIX architecture presented in this paper illustrates how data justice principles, articulated in the HDI framework, can be translated into a MAS architecture formulated around the *DataAgent* to provide *legibility, agency*, and *negotiability*; which is framed in terms of improved access control to and contextual integrity of personal health data. Some of the solutions that have been proposed for this challenge include MeD-lights, a system that uses the traffic light metaphor (i.e., red, yellow, green) to indicate and label the sensitivity levels of personal health data (Adams, Intwala, & Kapadia, 2010). The MeD-lights system provides a mechanism for an intuitive specification of the privacy and confidentiality requirements associated with personal health data. In this solution, the challenge of forfeiting control, at a technology level, once data is shared, is not addressed.

Mortier *et al.* (2014) have proposed the concept of a databox, initially conceived as a distributed system for the federation of personal health data, providing APIs to access data held in the personal databoxes, and fundamentally moving the code

and processing to data, such that only results of the requested computation are communicated to third parties, without releasing personal data. The design of the databox is informed by the requirements for it to be a trusted platform, to provide for data management, enabled controlled access, and to enable incentives for all parties. While the databox in this solution has some similarities to the functionality of the *DataAgent*, the primary difference is that the databox provides a federated repository to various data sources and accepts code requests for execution on the personal data. The *DataAgent* provides data sharing through agent mobility, which is coupled with the functionality to manage the use of the data within the specific context.

The PHIX architecture is consistent with both the digital phenotype perspective (Loi, 2019), as well as the notion of a digital/virtual 'data double' that is endowed with both data and functionality. Invariably, the proposed architecture is framed to deal with a particular narrowly-defined scenario (i.e., sharing of personal health informatics data with a health service provider) and as such neglects some of the challenges associated in personal health informatics, such as N-dimensional attribute of data associated with the social and communal ownership of data.

CONCLUSION

The use of technology and data in society needs to be on terms that are consistent with the ethics and social justice values of a society. This research focused on the digital health domain and explored the key benefits and challenges associated with the use of ICTs and data technologies in health. It further investigates how the principles of social justice, encapsulated in the notion of data justice, can be outworked not only in the broad digital health data assemblages but also in health informatics technologies. As far as digital health and health informatics are concerned, the data justice principles encapsulated in frameworks such as the HDI, stand to provide guidelines that can inform the development and implementation of digital health technology solutions. Operationalizing such social justice and ethical principles is non-trivial and requires that the principles are translated and decomposed into specific constitutive system requirements. This paper has explored and presented an investigation of data justice in health informatics and has suggested the operationalization of the HDI *negotiability* requirements of (perpetual) control and contextual integrity through a MAS-based PHIX architecture that encapsulates individuals' data in a dynamic, mobile, virtual 'data double' *DataAgent* component. Such technology design artifacts, not only facilitate the standardization, mainstreaming, and embedding of normative societal values (e.g., social justice) in technology solutions, they also support the necessary operationalization of ethical frameworks and standards.

REFERENCES

Adams, E. K., Intwala, M., & Kapadia, A. (2010). MeD-Lights: A Usable Metaphor for Patient Controlled Access to Electronic Health Records. *Proceedings of the 1st ACM International Health Informatics Symposium*. doi:10.1145/1882992.1883112

Asilomar, A. I. (2017). *Principles*. Retrieved March 1, 2020, from https://futureoflife.org/ai-principles/

Bellifemine, F., Poggi, A., & Rimassa, G. (1999). JADE – A FIPA-compliant Agent Framework. *Fourth International Conference on Practical Application of Intelligent Agents and Multi-Agent Technology (PAAM 1999)*, 97–108.

Boyd, D., & Crawford, K. (2012). Critical Questions for Big Data. *Information Communication and Society*, *15*(5), 662–679. doi:10.1080/1369118X.2012.678878

Burrell, J. (2016). How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, *3*(1), 205395171562251. doi:10.1177/2053951715622512

Busch, L. (2011). *Standards: Recipes for Reality*. 10.7551/mitpress/8962.001.0001

Crawford, K., Lingel, J., & Karppi, T. (2015). Our metrics, ourselves: A hundred years of self-tracking from the weight scale to the wrist wearable device. *European Journal of Cultural Studies*, *18*(4–5), 479–496. doi:10.1177/1367549415584857

Haggerty, D., Richard, V., & Ericson, K. (2000). The surveillant assemblage. *The British Journal of Sociology*, *51*(4), 605–622. doi:10.1080/00071310020015280 PMID:11140886

Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.-H., Metayer, D. Le, Tirtea, R., & Schiffner, S. (2015). *Privacy and Data Protection by Design - from policy to engineering*. 10.2824/38623

Data Ethics Framework. (2018). Retrieved from https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework

De Vries, H., Jakobs, K., Egyedi, T., Eto, M., Fertig, S., Kanevskaia, O., Klintner, L., Koch, C., Mijatovic, I., Mirtsch, M., Morone, P., Orviska, M., Riillo, C., & Scaramuzzino, G. (2018). Standardization: Towards an agenda for research. *International Journal of Standardization Research*, *16*(1), 52–59. doi:10.4018/IJSR.2018010104

Dencik, L., Hintz, A., & Cable, J. (2016). Towards data justice? The ambiguity of anti-surveillance resistance in political activism. *Big Data & Society*, *3*(2), 205395171667967. doi:10.1177/2053951716679678

Epstein, D. A., Ping, A., Fogarty, J., & Munson, S. A. (2015). A lived informatics model of personal informatics. *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing - UbiComp '15*, 731–742. doi:10.1145/2750858.2804250

Ethical O. S. Toolkit. (2005). Retrieved February 25, 2019, from https://ethicalos.org/

Fernandez, E., Ajaj, O., Budkley, I., Delessy-Gassant, N., Hashizume, K., & Larrondo-Petrie, M. (2012). A survey of patterns for web services security and reliability standards. *Future Internet*, *4*(2), 430–450. doi:10.3390/fi4020430

Fleck, R., & Harrison, D. (2015). Shared PI: Sharing personal data to support reflection and behaviour change. *Workshop on" Beyond Personal Informatics: Designing for Experiences of Data"- CHI2015*.

Floridi, L. (2014). *The 4th revolution : how the infosphere is reshaping human reality*. Oxford University Press.

Gardiyawasam Pussewalage, H. S., & Oleshchuk, V. A. (2016). Privacy preserving mechanisms for enforcing security and privacy requirements in E-health solutions. *International Journal of Information Management*, *36*(6), 1161–1173. doi:10.1016/j.ijinfomgt.2016.07.006

Harris, C. E. Jr. (2008). The good engineer: Giving virtue its due in engineering ethics. *Science and Engineering Ethics*, *14*(2), 153–164. doi:10.1007/s11948-008-9068-3 PMID:18461475

Heeks, R., & Renken, J. (2018). Data justice for development. *Information Development*, *34*(1), 90–102. doi:10.1177/0266666916678282

Henwood, F., Wyatt, S., Hart, A., & Smith, J. (2003). "Ignorance is bliss sometimes": Constraints on the emergence of the "informed patient" in the changing landscapes of health information. *Sociology of Health & Illness*, *25*(6), 589–607. doi:10.1111/1467-9566.00360

ISO/IEC. (2011). *ISO/IEC 29100:2011 Information technology — Security techniques — Privacy framework*. Retrieved March 1, 2020, from https://www.iso.org/standard/45123.html

ISO. (2019). *Consumers and Standards: Partnership for a Better World*. Retrieved March 1, 2020, from https://www.iso.org/sites/ConsumersStandards/index.html

Jacobs, B., & Popma, J. (2019). Medical research, Big Data and the need for privacy by design. *Big Data & Society*, *6*(1), 205395171882435. doi:10.1177/2053951718824352

Jakobs, K. (2019). ICT Standardization. In *Advanced Methodologies and Technologies in Artificial Intelligence* (pp. 812–825). Computer Simulation, and Human-Computer Interaction. doi:10.4018/978-1-5225-7368-5.ch060

Johnson, J. (2016). The question of information justice. *Communications of the ACM*, *59*(3), 27–29. doi:10.1145/2879878

Knoppers, B. M., & Thorogood, A. M. (2017). Ethics and Big Data in health. *Current Opinion in Systems Biology*, *4*, 53–57. doi:10.1016/j.coisb.2017.07.001

Lapouchnian, A. (2005). Goal-Oriented Requirements Engineering : An Overview of the Current Research. *Requirements Engineering*, *8*(3), 32. doi:10.1007/s00766-003-0178-9

Li, I., Dey, A., & Forlizzi, J. (2010). A stage-based model of personal informatics systems. *Proceedings of the 28th International Conference on Human Factors in Computing Systems - CHI '10*, 557. doi:10.1145/1753326.1753409

Loi, M. (2019). The Digital Phenotype: A Philosophical and Ethical Exploration. *Philosophy & Technology*, *32*(1), 155–171. doi:10.1007/s13347-018-0319-1

Lupton, D. (2013). The digitally engaged patient: Self-monitoring and self-care in the digital health era. *Social Theory & Health*, *11*(3), 256–270. doi:10.1057/sth.2013.10

Mai, J.-E. (2016). Big data privacy: The datafication of personal information. *The Information Society*, *32*(3), 192–199. doi:10.1080/01972243.2016.1153010

Marcengo, A., & Rapp, A. (2014). Visualization of human behavior data: The quantified self. *Innovative Approaches of Data Visualization and Visual Analytics*, *1*, 236–265. doi:10.4018/978-1-4666-4309-3.ch012

Morley, J., & Floridi, L. (2019). The Limits of Empowerment: How to Reframe the Role of mHealth Tools in the Healthcare Ecosystem. *Science and Engineering Ethics*, (0123456789). Advance online publication. doi:10.1007/s11948-019-00115-1 PMID:31172424

Mortier, R., Haddadi, H., Henderson, T., McAuley, D., & Crowcroft, J. (2014). Human-Data Interaction: The Human Face of the Data-Driven Society. SSRN *Electronic Journal*. 10.2139/ssrn.2508051

Nambiar, S. (2013). Capabilities, conversion factors and institutions. *Progress in Development Studies*, *13*(3), 221–230. doi:10.1177/1464993413486547

Nissenbaum, H. F. (2010). *Privacy in context : technology, policy, and the integrity of social life*. Stanford Law Books.

Postman, N. (2013). Informing ourselves to death. In D. S. Niederhauser, J. K. Olson, & M. P. Clough (Eds.), *The nature of technology* (pp. 5–14). doi:10.1007/978-94-6209-269-3_2

Prochaska, J. O., & Velicer, W. F. (1997). The Transtheoretical Model of Health Behavior Change. *American Journal of Health Promotion*, *12*(1), 38–48. doi:10.4278/0890-1171-12.1.38 PMID:10170434

Puussaar, A., Clear, A., & Wright, P. (2017). Better together: Reciprocal sharing and social sensemaking of data. *Workshop on "Quantified Data and Social Relationships" -CHI2017*.

Rooksby, J., Rost, M., Morrison, A., Chalmers, M. C., Rooksby, J., Rost, M., & Chalmers, M. C. et al. (2014). Personal tracking as lived informatics. *Proceedings of the 32nd Annual ACM Conference on Human Factors in Computing Systems - CHI '14*, 1163–1172. doi:10.1145/2556288.2557039

Ruger, J. P. (2006). Toward a Theory of a Right to Health: Capability and Incompletely Theorized Agreements. *Yale Journal of Law & the Humanities*, *18*(2), 3. https://www.ncbi.nlm.nih.gov/pubmed/25309105 PMID:25309105

Sharon, T. (2018). When digital health meets digital capitalism, how many common goods are at stake? *Big Data & Society*, *5*(2), 205395171881903. doi:10.1177/2053951718819032

Stals, S., Smyth, M., & Mival, O. (2017). Sharing and exploring Quantified-Self Data on In-Place experiences and emotions. *ACM CHI 2017 - Quantified Data and Social Relationships*.

Sterckx, S., Cockbain, J., Howard, H., Huys, I., & Borry, P. (2013). "Trust is not something you can reclaim easily": Patenting in the field of direct-to-consumer genetic testing. *Genetics in Medicine*, *15*(5), 382–387. doi:10.1038/gim.2012.143 PMID:23174801

Taylor, L. (2017). What is data justice? The case for connecting digital rights and freedoms globally. *Big Data & Society*, *4*(2), 205395171773633. doi:10.1177/2053951717736335

Wickson, F., & Forsberg, E. M. (2015). Standardising Responsibility? The Significance of Interstitial Spaces. *Science and Engineering Ethics*, *21*(5), 1159–1180. doi:10.1007/s11948-014-9602-4 PMID:25344842

Woolley, J. P., McGowan, M. L., Teare, H. J. A., Coathup, V., Fishman, J. R., Settersten, R. A. Jr, Sterckx, S., Kaye, J., & Juengst, E. T. (2016). Citizen science or scientific citizenship? Disentangling the uses of public engagement rhetoric in national research initiatives. *BMC Medical Ethics*, *17*(1), 33. doi:10.1186/s12910-016-0117-1 PMID:27260081

World Health Organization. (2018). Resolution WHA71.7. *Resolutions and Deliberations on EHealth*. Retrieved from https://www.who.int/news-room/detail/25-05-2018-seventy-first-world-health-assembly-update-25-may%0Ahttp://apps.who.int/gb/ebwha/pdf_files/WHA71/A71_R7-en.pdf?ua=1

Zuboff, S. (2015). Big other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology*, *30*(1), 75–89. doi:10.1057/jit.2015.5

Mamello Thinyane is passionate about the potential of scientific research and technology innovation to contribute to the achievement of sustainable good life for all. He is a Principal Research Fellow at the United Nations University Institute in Macau, where he leads research within the Data and Sustainable Development group, formerly the Small Data Lab. His work focuses on the role of data and technology for enhancing the engagement and participation of civil society stakeholders towards the achievement of sustainable development goals. Before joining UNU, Mamello was an Associate Professor in the Department of Computer Science at the University of Fort Hare in South Africa, as well as the Director for the Telkom Centre of Excellence in ICT for Development at the same institute. He is the Associate Editor of the Journal of Technology in Human Services and a Conference Co-chair for the 11th International Development Informatics Association (IDIA2020) conference. Mamello holds a PhD in Computer Science from Rhodes University.