THE FUTURES OF EHEALTH

Social, Ethical and Legal Challenges

Edited by
Thomas Christian Bächle and Alina Wernick

ALEXANDER VON HUMBOLDT INSTITUTE FOR INTERNET AND SOCIETY, BERLIN, GERMANY

The Alexander von Humboldt Institute for Internet and Society (HIIG) explores the dynamic relationship between the Internet and society, including the increasing penetration of digital infrastructures into various domains of everyday life. Its goal is to understand the interplay of social-cultural, legal, economic, and technical norms in the process of digitisation.

Alexander von Humboldt
INSTITUTE FOR INTERNET
AND SOCIETY

CONTENTS

TECHNOLOGY AND INNOVATION IN CONTEXT

EHEALTH IN PRACTICE – CASE STUDIES

EHEALTH AND THE LAW: COMPARATIVE PERSPECTIVES

The futures of eHealth – introducing the social, legal and ethical challenges

THOMAS CHRISTIAN BÄCHLE AND ALINA WERNICK

Looking into the futures of eHealth? The title of this publication might seem quite presumptuous at first. Its objective, however, is to serve a much more modest purpose, in that it strives to take a look at potential, likely, desired, anticipated or feared futures of digital health technologies and practices. When analysing the opportunities and risks associated with them as well as the social, legal and ethical challenges they might pose, what we also see in the process are the expectations and promises projected onto them.

eHealth or "digital health", according to the World Health Organization's European Office, "involves a broad group of activities that use electronic means to deliver health-related information, resources and services: it is the use of information and communication technologies for health" (World Health Organization 2017). As far as current developments and technological solutions are concerned, the WHO has further identified the following areas:

- Electronic health records and interoperability of data;
- Mobile health or mHealth;
- Telehealth, where a patient can consult with a healthcare worker using Skype or even a regular telephone;
- Wearable technologies (fitness trackers, medical devices, etc.) and
- Technologies to support integrated care (WHO 2017).

Looking into the futures of anything always involves creating narratives. Rather unsurprisingly, the WHO's definition characterises the role of technology use as entailing "strengthening health systems and health information systems" (World Health Organization 2017), a narrative of opportunity. These promises of eHealth are embedded in and reflective of much larger discourses that are often associated with (digital) technologies, which are mainly seen as a remedy to existing social problems. These discourses often centre around terms such as "empowerment", "democratic potential", "unifying cross-border force", "special care for vulnerable groups" or "bridging distances". And, indeed, there is an abundance of opportunities in digital health solutions that are directly associated with these technologies and practices.

From a *patient perspective*, eHealth makes the promises of improved access to medical services or of individualised medicine via targeted treatments (e.g. patient-specific cancer therapies). It is characterised as enabling patients' self-management and helping them to reach informed decisions.

DOI: 10.5281/zenodo.3296733

From a *medical perspective*, one of the opportunities associated with eHealth is that it will speed up the process of implementing medical research findings in healthcare practices, involving all relevant fields from diagnostics and therapies to technological devices and decision-making processes. Among the objectives - and the promises - of digital healthcare are that it will bring about generally improved patient outcomes while enhancing safety and reducing medical error. Telemedical services are expected to facilitate healthcare delivery and provide access to medical expertise in rural areas, across nations or even across continents. eHealth is expected to help reduce expenses and to solve major problems associated with an aging population or rare and chronic diseases. Furthermore, the implementation of innovative data analytics methods into health systems should allow for developments such as predictive diagnostics – anticipating future ailments and allowing timely intervention – and "individualised precision medicine".

These last points – precision, prediction and individualisation – also raise hopes and expectations from a *research perspective*, hopes that are mainly associated with the well-known promises of "Big Data" (e.g. Mayer-Schönberger/Cukier 2013) for research processes and scientific evidence. These promises, however, have sparked considerable criticism in recent years, since they often assume a "more objective" type of knowledge. Data-rich environments imply gaining access to all the data there is (not just to medical data but also to social and cultural information on individuals) and analysing it via efficient machine learning methods (so-called artificial intelligence). This idea of a universal representation of all potentially relevant factors has been persuasively applied in various fields such as genomics, biomarkers, biosocial parameters or gene-environment interaction. Experiments and causality-based research, it has been claimed, will become obsolete and be succeeded by correlation, salient patterns or computer simulations. This promise expands to creating probability-based knowledge about future scenarios in the above-mentioned field of predictive diagnostics.

Of course, the debates also give voice to critical discourses concerning the risks associated with "the invasion and loss of privacy", "surveillance and control" or "automation" accompanied by the feared "loss of human agency"; this begs the question of how we can ensure that patients receive good care via these technologies, how the technologies can help doctors and medical professionals and how we can prevent them from causing harm or violating individual freedoms. Also, there are many additional challenges, including the cost of the equipment, the lack of necessary infrastructure, and the need to train doctors, medical staff and also patients. The positive effects of digital health are directly linked to media and data literacy as well as to technology acceptance.

Finding answers to these issues is highly complex and involves both social and cultural as well as legal questions and challenges that in many instances are highly interwoven with each other.

SOCIAL AND CULTURAL CHALLENGES AND QUESTIONS

As scholars consider developments in the field of eHealth as part of the extensive social and cultural transformations brought about by digitalisation, a more nuanced picture is emerging. Among the most relevant questions and pressing issues are:

(1) The tendency towards *universal datafication*: the seemingly all-encompassing collection of data in all areas of life is leading to a structural loss of privacy, a value that is deeply rooted in Western modernity. It has been succeeded and challenged by a much more fluid understanding of what is private and what is public, which is particularly relevant for the highly sensitive area of information on health (Nissenbaum 2010). Besides obviously medically relevant data (such as biochemical and genetic information), it is a wide range of data on social and cultural parameters (such as group affiliation, location and movement, consumer behaviour etc.) that are being taken into account when making correlation-based assertions about their relevance for an individual's present and future health. Given all the digital traces we leave in our everyday lives, virtually any piece of information might become medically relevant. Once the data is there, it is very difficult not to use it. The risks are obvious and pertain to issues such as data protection and confidentiality, a tendency to overdiagnosis, or the danger of producing "false" knowledge either involuntarily through chance correlations or even deliberately by outright manipulation of data.

(2) The tendency towards a *universal valorisation of data*: one of the most serious side effects of data collection by communication and tracking devices is that is large and powerful technology companies that gain easy access to them. It is a truism that sensitive data – including medically relevant data – are essential for the new business models that have emerged around virtually all types of personal data. Once the data is there, it is difficult not to make money with it. Monetising personal data has become a norm, both for companies and their users, who appreciate the "free" services they offer. Strangely, as part of this norm, being transparent about your own data has been established as the default. Consequently, protecting your own personal data becomes an opt-in and might eventually be offered to you as an additional service that you either can or cannot afford. An increasing commercialisation of health data risks reinforcing social and economic divides if the affluent are able to pay for any service they want and keep their data private and secure in the process while the less affluent either pay with their data (e.g. when a discount is given to patients when they make their data transparent) or are paid off when "donating" their data. This may not only be a problem within national health services but also on a global scale, for instance, if richer countries "extract" medically relevant data from poorer regions of the world with more lenient data protection legislation or greater economic need.

(3) Does eHealth lead to a more *personalised* or to more *de-personalised healthcare*? Does it foster *patient autonomy* or is it means of *patient surveillance* and *control*? For both questions, the picture is very complex and the answers are never either/or. Data is becoming central in diagnostics and patient therapy because they promise to provide more effective, individualised care. But at the same time, there is a real risk that patients may no longer be regarded holistically but as mere bearers of medically (ir)relevant data, which is the product of (self-)monitoring and automated data analysis. These tendencies might even lead to an increased de-personalisation of individual patients by reducing the quantity and quality of human contact in doctor-patient relationships. Closely interwoven with this development is the focus on the individual: digital health does not just make medical expert knowledge more available and accessible; with devices such as self-trackers or electronic diagnostic tools, it can also empower patients and ensure a higher degree of autonomy. At the same time, the flipside of this higher degree of self-determination is a potentially ubiquitous culture of medical (self-)surveillance, with control not only being exercised from without but from within: it becomes the individual's responsibility to stay healthy by looking after and optimising his or her own lifestyle, nutrition or level of exercise.

GENERAL LEGAL RESEARCH PERSPECTIVES

(1) The central legal challenge surrounding eHealth is legal uncertainty, which has multiple origins. Health law – which regulates patients' rights to healthcare, health insurances and healthcare professions – has traditionally been regarded as *a complex field of law*. It is challenging to interweave innovation and technological progress in the healthcare field with existing health law. This is evident internationally in initiatives to regulate the use of electronic health records. For example, in Germany, where healthcare is provided by a large number of private and public actors, enabling the seamless use of electronic health records is a tedious process. The complexity of health law is also evident in the reimbursement of telemedicine. EU law mandates that cross-border telemedical services be reimbursed when they are also covered by the patient's national health insurance. However, it can be difficult for patients to find out what their insurance coverage for telemedical services is. Expanding the range of reimbursable telemedical services so that they are on a par with in-person medical services would foster the adoption of telemedicine.

The complexity of health law is also reflected in the discussion on informed consent, and questions arise as to whether users of eHealth services are sufficiently informed about how their data is processed by eHealth technology providers. However, users of eHealth technologies, who are often patients, must in many cases give multiple different permissions, each of which has a distinct legal significance: consent to processing personal data,

to disclosing information subject to professional secrecy, to receiving treatment and to taking part in medical research, including clinical trials. Furthermore, the conditions for giving consent depend on the purpose of data processing and the jurisdiction in question.

(2) Existing *legal frameworks may not fit seamlessly with novel technologies*. For example, the standard for liability is different depending on whether the damage is caused by hardware, software or a healthcare professional. As a consequence, users of eHealth apps that bring together multiple technologies and services may find it difficult to determine what their rights are when something goes wrong. Even though the Medical Device Regulation applies to software with a specific medical purpose (Art. 2 (1)), wellness apps fall outside its scope, which may require attention from the field of consumer law.

(3) Often *existing laws may be silent* with respect to eHealth technologies, such as telemedicine, mHealth or AI-based applications. New legislation may prove necessary to increase their adoption or to ensure their safe use. For example, Russia, Brazil, the US and Germany have recently changed their legislation on telemedicine, and AI regulation has been subject to heated global debate. In some situations, existing laws may not even cover certain ethical challenges associated with eHealth technology. For example, the use and sale of anonymised health data may be perfectly legal but nevertheless raise ethical problems, for example, in terms of how they may inform insurance or marketing policies.

(4) Legal uncertainty increases whenever eHealth is applied in *a cross-border context*. In the EU, both health law and tort and contract law are not harmonised, and may differ dramatically between EU member states. In Germany, the relevant legislation is at least partly a state matter. Given that the healthcare systems across the EU are very diverse, patients, healthcare professionals and service providers operate in a very complex legal landscape, especially when services are offered across member states' borders. Furthermore, eHealth is an international phenomenon, and technologies such as telemedicine make it possible to treat patients who may be located on other continents. As a consequence, it is difficult to introduce eHealth products and services on an international scale without substantial investment to ensure legal compliance.

(5) *Harmonisation of legislation is not a panacea* for legal uncertainty, as can be seen from the General Data Protection Regulation (GDPR), which came into force in 2018. The digitalisation of healthcare, the popularity of mHealth applications and the prevalence of self-tracking technologies are all powered by processing health data, which is deemed sensitive under the GDPR (Art. 9). However, the GDPR does not fully harmonise the law on data protection in Europe. In fact, its rules on processing health data contain several references to national legislation. For example, professional confidentiality requirements for healthcare professionals remain regulated on the national level and are often subject to different standards of liability. In the EU, the legislation on healthcare remains in the competence of member states and is hence outside the scope of EU law.

However, even within this very heterogeneous legal landscape, many of the challenges associated with eHealth are similar across the world. Engagement in interdisciplinary, comparative dialogue with an international focus is a step towards alleviating the legal uncertainties associated with eHealth. This may enable eHealth providers to operate in the current, complex legal landscape and help to regulate the use of future eHealth technologies in a manner that is legally, socially and ethically sustainable. Through dialogue, we can learn from solutions adopted in other countries and identify the best regulatory and policy measures for eHealth.

Researchers from various countries and disciplines discussed these issues at the international and interdisciplinary conference "The Futures of eHealth. Social, Legal and Ethical Challenges", which was held on 29 and 30 April 2019 in Berlin, Germany. This publication identifies and details the social, legal and ethical opportunities, risks, benefits and challenges of innovative digital health technologies.

OVERVIEW OF THE CONTRIBUTIONS

The first section provides an overview of *Current Challenges in eHealth*. Arguing that mobile health applications blur traditional sector boundaries and consequently challenge research on health ethics, the *META research group* concludes in their paper that a "responsible, socially and globally sustainable and user-centric innovation" is of prime concern in order to uphold values such as patient empowerment, democratisation and procedural improvements in health and health care. *Valeska Cappel* and *Karolin Kappler* also focus on mobile health applications and shed light on potential lines of conflict in their development, implementation and diffusion by comparing the underlying conventions, investments in form and practices of different stakeholders. From a legal perspective, *Trix Mulder* looks at the principle of informed consent in the context of European data protection laws. She argues that the privacy policies of health apps and wearables are not always clear on the purposes for processing, which can result in the loss of purpose limitation as a safeguard for data protection. *Thomas Christian Bächle* looks at the ethical challenges that arise with innovations in the field of digital health, namely around developments such as universal data collection, machine learning analytics (so-called AI) and automated decision-making. These entail complex questions on shared agency and distributed responsibility as well as patient autonomy and social sorting.

The second section focuses on the *Uses and Perceptions of eHealth Applications*. *Freya Sukalla and Veronika Karnowski* analyse the portrayal of mental well-being apps in the smartphone app market, which are often categorised using keywords such as lifestyle instead of health, fitness or medicine. They find that these apps and the ways they are represented implicitly promote the idea of sole individual responsibility for well-being

and mental health, which leads them to conclude that this may have serious negative implications, including exacerbating stigmatisation. *Isabell Koinig and Sandra Diehl* look at wearable and self-tracking technologies in the context of lifelogging, personal fitness and empowerment. In particular, they ask to what degree evaluations of an advertisement for a wearable product are influenced by individuals' attitudes towards fitness and their interest in new technologies. While self-tracking clearly articulates power structures, the authors frame the concept of empowerment in the context of marketing: how can it be made known to people that new technologies in the field of eHealth can be beneficial for their health? *Galit Madar, Azi Lev-On and Nachman Ash* analyse the changing images of family physicians as perceived by their patients who use eHealth systems, as well as patients' perceptions of their interactions with their physicians in an Israeli context. Their findings indicate that physicians believe that the introduction of eHealth systems significantly transformed what we term the professional, interpersonal, and therapeutic aspects of their image as family physicians. The section concludes with a summary – authored by *Niklas Trinkhaus – of Btihaj Ajana's* keynote entitled "Self-management for better health? Reflections on the self-tracking culture", which she delivered at the conference on 30 April 2019 in Berlin. She argues that while the growing self-tracking culture was expected to be part of the solution to severe problems in the public health sector, the promises of a personalised, participatory and preventive approach towards health cannot live up to expectations. Even though some benefits and positive outcomes of self-tracking can be identified, she warns of excessive optimism regarding the potential of self-tracking technologies.

The third section, *Technology and Innovation in Context*, begins with *Martin Stojanov's* study on second-order data interoperability in public health, which highlights the challenges of repurposing web-based data and measures that need to be undertaken to ensure interoperability. *Anastasiya Kiseleva* discusses the transparency of AI-made decisions in healthcare, stressing the importance and need for legislative measures that maintain trust in AI-facilitated medical treatment. *Irma Klünker's* report on the Markets for eHealth panel discussion features the perspectives of innovators and entrepreneurs operating in the eHealth sector. The panel raised awareness about the challenges entrepreneurs face in Germany and the UK when introducing eHealth services to the market, such as the complexity of the healthcare sector and the struggle to acquire funding and ensure legal compliance, especially with respect to data. The challenges of eHealth are global, and the panel discussion curated by Asia eHealth Information Network (AeHIN) on the international perspectives brought understanding of the efforts to adopt eHealth technology in Asia, South America and Africa and Europe. The report on the panel, written by *Niklas Trinkhaus*, identifies interoperability, international cooperation and the prevention of abuses of health data as important challenges in the development of eHealth when seeking to achieve the UN goal of *universal health coverage*.

The section *eHealth in Practice* presents international case studies on the various ways digital health technologies are being used, detailing social contexts, challenges and benefits. *Daniela Rudner, Lynda Toussaint and Nao Sipula* introduce Unjani Clinic, a social franchising initiative in South Africa that has created a primary healthcare container clinic network in underserved areas. In particular, they highlight the role of electronic health records and telehealth as technological solutions applied in this project. *Manisha Mantri, R. Rajamenakshi and Gaur Sunder* look at the extensive digitisation of the health sector and highlight major issues in the debate on policies, regulations and technical standards. With respect to data privacy, they argue that additional attention must be given to the handling of patients' health data, including both legal and ethical aspects, and they explore the initiatives on policies, regulations and technical standards. *Arun Shroff* discusses a diagnostic tool that enables the early detection of diabetic retinopathy (DR) using so-called artificial intelligence that is being deployed and tested in India. DR is a serious eye-disease that affects over 148 million people worldwide and can lead to vision impairment and vision loss if it is not detected and treated early enough. It is argued that this method of automatically screening retinal images offers an effective alternative to human diagnosticians, since there are not enough specialists worldwide to screen everyone at risk. The paper outlines the objectives of the project as well as the challenges faced.

The section begins with *Stefaan Callens'* review of the current and upcoming legal challenges in eHealth that call for regulatory initiatives by the EU: transparency in the multiparty processing of health data, clinical assessment of health technologies, enablement of multiparty, interstate cooperation and information exchange for the provision of telemonitoring services, removing legal obstacles of the adoption of cross-border medicine and ensuring pro-competitiveness of big data and AI. In her paper on the secondary use of data in the context of medical research, *Paola Aurucci* discusses the complex interplay of data protection law and clinical trial regulations, both of which address the use of health related data. The power of EU member states to enact stricter legislation in connection with sensitive data may lead to situations in which medical research is undertaken in considerable uncertainty about how to process health-related data in a legally compliant manner.

Mikhail Zhuravlev reviews the recent Russian legislation on eHealth, which addresses the use of electronic health records and telemedicine. In Russia, the criteria for giving informed consent for the processing of health data are strict, formal and burdensome to meet in the context of eHealth. Besides the legislation on the processing of health data, other legislative solutions also have an impact on the adoption of eHealth technology. *Lauren Tonti* investigates the conditions under which telemental health is reimbursed in France, Australia and the Netherlands, stressing the importance of parity – the reimbursement of telemental care services on a par with face-to-face health care. She highlights the need to codify parity policies in law.

Especially in countries with large rural populations, telehealth can facilitate access to healthcare. Of all the legal norms addressing telemedicine, those that directly prohibit or limit long-distance treatment have the most pronounced effect on its adoption. *Alina Wernick* and *Irma Klünker* review the historical background and current status of the prohibitions and limitations on long-distance treatment in Germany and in the US, arguing in favour of evidence-based regulation that ensures the delivery of safe medical care in view of the advances of telemedical technology. *Mariana Canto* discusses the development of a telehealth policy in Brazil and the challenges in regulating data protection, privacy and cybersecurity of telehealth as well as the conditions for accessing it, bearing in mind the social and economic aspects of telehealth delivery.

Our publication ends with a collection of *#eHealthFutures2040* predictions shared by our conference participants. Whereas the conference presentations looked a few years ahead into the future developments of eHealth, the conference participants were asked to share their predictions about eHealth in 2040.

ACKNOWLEDGEMENTS

The editors want to thank all participants for making the conference an insightful, multifaceted and prolific event. In particular, our thanks go to the presenters for their efforts in offering their contributions for publication in this edited volume. This ensures that their valuable research results can be shared with a broader public.

We also wish to thank the keynote speakers Btihaj Ajana (King's College London) and Stefaan Callens (Catholic University of Leuven) for their inspiring talks as well as the chairs of the panel discussions, Elif Kücüktas and Janis Reinelt, for their effort and dedication. We are grateful to our panellists, who enriched our understanding of eHealth by bringing in their perspectives on innovation and business, international initiatives and ethical questions in the field of eHealth. We also want to thank the Berlin Institute of Health, our network partner for the conference.

It is with heartfelt gratitude that we acknowledge the work and effort of Jai Ganesh Udayasankaran of AeHIN for curating an outstanding panel on "International Perspectives on eHealth Policies", the members of which represented four different continents.

We are also thankful to the Humboldt Institute's great event management team and the many people who were involved in organising the conference, in particular (and in alphabetical order): Christian Grauvogel, Irma Klünker, Natalie Kreindlina, Ronja Lamberty, Marc Pirogan and Niklas Trinkhaus. Our thanks also go to Roisin Cronin, Katja Margulis and Larissa Wunderlich for their excellent work in language revision as well as in visualising, typesetting and laying out this publication.

The editors are particularly grateful to Thomas Schildhauer, who initiated our project on the topic of eHealth ("The Futures of Telemedicine"). Without him, neither the conference nor this edited volume would have seen the light of day. We also want to thank the Silicon Valley Community Foundation for funding this project through a research fund provided by Cisco Systems.

BIBLIOGRAPHY

Mayer-Schönberger, V., & Cukier, K. (2013). *Big Data. A Revolution that Will Transform How We Live, Work and Think.* London: John Murray.

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Chicago: University of Chicago Press.

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).

Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC.

World Health Organization (2017). *eHealth - where are we now?*. Retrieved from: http://www.euro.who.int/en/health-topics/Health-systems/e-health/ehealth-where-are-we-now, (last accessed: 10.05.2019).

CURRENT CHALLENGES IN EHEALTH

Ethical, legal and social aspects of mHealth technologies: Navigating the field

THE META RESEARCH GROUP
VERINA WILD, SARAH AKGÜL, KATHARINA EISENHUT, TEREZA HENDL, BIANCA JANSKY, FELIX MACHLEID, NIELS NIJSINGH, NICOLE PETER AND ELA SAUERBORN

mHealth blurs health sector boundaries, challenging health ethics research: a dynamic approach and curiosity for tech innovation is needed.

Keywords: mobile health technologies, ELSA research, complexity, responsible innovation, interdisciplinarity

INTRODUCTION

Mobile health (mHealth) technologies, such as apps, smartwatches, sensors or technology built into shoes or fabrics, are increasingly becoming an essential part of healthy lifestyles, disease prevention and management. The hope is that mHealth can revolutionise and transform healthcare (European Commission 2014, 2018; WHO 2011).

Given the ground-breaking importance for health and health care mHealth is assumed to have, our research team "META"[1] interrogates the ethical, legal and social aspects (ELSA) of mHealth. In this article, we identify some profound and potentially conflicting implications of mHealth for individuals and society. In our conclusion, we emphasise the importance of rethinking disciplinary and normative approaches to mHealth.

INCREASES IN SELF-EMPOWERMENT, HEALTH BENEFITS AND EFFICIENCY

A significant part of the transformative potential of mHealth is seen in its participatory and empowering effects, which will likely lead to increased user autonomy and a democratisation of healthcare. With the help of various digital technological features, the roles of users (i.e. healthy individuals and patients) are shifting towards more active participa-

[1] Acronym for: "mHealth: Ethical, legal and social aspects in the technological age". The project is funded by the German Ministry of Education and Research, and runs from April 2018 to March 2024 (Grant number: 01GP1791). In an interdisciplinary team with expertise in philosophy, bioethics, public health ethics, sociology, law, gender studies, public health and medicine, we have undertaken empirical and conceptual research since April 2018.

DOI: 10.5281/zenodo.3296853

tion in the maintenance and improvement of their own health, and away from oversight by health professionals or the healthcare system (Swan 2012). mHealth thus challenges conventional hierarchies in healthcare (Kingod 2018); patients are no longer "passive recipients of care" (Lewis & Leibrand 2016); they become "digitally engaged" (Lupton 2013d). Health-related knowledge is no longer concentrated within the boundaries of medical facilities or in the hands of medical experts. In this narrative, mHealth users are empowered to be in charge of their health and to personally improve it.

The hope is that mHealth can positively influence disease management, prevention and health promotion, as well as access to health care (Kreps & Neuhauser 2010, Ospina-Pinillos et al., 2018). There are demonstrable benefits of its use for example in areas of surveillance and mapping of malaria infection patterns (Brownstein 2009, Fornace 2018), prenatal care for asylum seekers (Borsari et al., 2018) or in relation to physical activity after prostatectomy (Agarwal et al. 2018). Some studies indicate that those who digitally track their own health are more likely to improve their health awareness and behaviour (Figueiredo et al. 2017). For example, one study has identified a positive short-term effect on smoking cessation (Uthman et al. 2019) and studies have shown that the use of mHealth increases individuals' health awareness, e.g. with respect to chronic diseases (Griauzde et al. 2019).

It has been argued that helpful factors in mHealth-facilitated behavioural changes include immediate graphical representations of body data, the ability to share information and the feeling of being part of a social network of users with similar experiences (Rönkkö 2018). Hopes for reducing harmful hierarchies and exclusionary processes have been associated with the use of the internet (Tierney et al. 2018), to which mHealth is connected. Furthermore, situationally relevant data available at all times have been found to help users and healthcare professionals to obtain a more detailed understanding of health and illness, enabling better-informed health decisions (Steinhubl et al. 2015).

Advocates of mHealth promote these technologies as the most promising drivers of solutions to pressing organisational and financial challenges in the healthcare sector (PwC 2013; Swan 2012). In their view, these technologies will facilitate increased effectiveness in implementing healthcare and prevention initiatives, a promotion of healthy lifestyles, improvements in international communication by health professionals, reductions in health inequalities and a personalisation of healthcare.

CHALLENGES: DATA, POWER, HEALTH AND JUSTICE

Despite these promising effects, there are significant challenges connected to mHealth. On a systemic level the "datafication of everything" (Mayer-Schönberger & Cukier 2013) is a significant and challenging issue. Some argue that the seemingly complete descrip-

tion of the reality given by peta- and exabytes of data is, in fact, never neutral but always a selective capture of reality only (Chang et al. 2014; Kitchin 2014). Scholars point out that digital technologies create an illusion of a comprehensive representation of reality, signifying a possible paradigm shift in knowledge and knowledge production (Chang et al. 2014; Kitchin 2014). Moreover, the selective representation of "reality" is shaped by normative assumptions about healthy lifestyles and social roles, which are fundamentally impacted by categories of power, such as gender, race or class (Hendl et al. 2019).

Just like data, algorithms are also never neutral, but carry with them certain dominant norms, values or concepts. The training data used to feed algorithms and the past data and definitions of success utilised by them can all be skewed by selective bias in data as well as by developers' personal values or prejudices (O'Neil 2016; AI NOW 2018). A resulting algorithmic bias can lead to misrepresentations of reality and have a negative impact on already structurally marginalised and disadvantaged groups (O'Neil 2016; Eubanks 2018; AI NOW 2018).

Further, data collection and control can bring about problematic power imbalances and increasingly asymmetric relationships between those who provide data and those who process and use it in large quantities (Ruckenstein & Schüll 2017; boyd & Crawford 2012, Lupton 2015b, Fangerau et al. 2016, Sharon 2016). For example, some point out that users of digital technologies do unpaid and invisible digital work (Ruckenstein & Schüll 2017), of which they might not be aware. By performing this work, users increasingly lose control over the data they create (Ruckenstein & Schüll 2017). Companies can monetise users' data, which is highly valued in the "healthcare market", which includes insurance companies (Nissenbaum & Patterson 2016: 98) along with other sectors such as marketing. Questions then arise as to how informed consent can be achieved or whether it is even possible to speak of informed consent when it is unclear how personal data will be processed, monetised or otherwise used (Fangerau et al. 2016).

Cyber-bullying or cyber-attacks (harmful hacking of devices) or data thievery are seen as additional risks (Belleken et al. 2016; Kotz 2011). Hacking and data misuse create new vulnerabilities within whole (sub)populations (Barnett et al., 2013). Malware and the intentional or unintentional manipulation of medical devices are also concerning and can cause e.g. unauthorised changes in the dosing of drugs (Khera 2017).

The increase in the self-tracking and "quantified self" movements are also being discussed critically. Such readings emphasise that potentially unrealistic body and health norms are being created, which can result in higher social pressures, disempowerment, exclusion or decreasing solidarity (Lupton 2014b; Sharon 2016, 2017). If mHealth generates constant surveillance, areas of human lives, such as nutrition, sexuality and (un-)healthy behaviour, can become associated with feelings of bad conscience, guilt and shame (Lupton 2015a). Kreitmair et al. (2017) argue that constant information updates can hinder productivity and have an addictive potential. Self-optimisation through

mHealth technologies could potentially cause depression in users, doing more harm than good (Fangerau et al. 2016; Hussain et al. 2017).

Technical difficulties can also jeopardise the necessary medical accuracy and reliability of mHealth data, for example, when instructions are not displayed correctly on a digital device by the patient or physician (Kreitmair et al. 2017). If mHealth applications misread body functions, such as heart rate, and give erroneous instructions, large groups of users may be misinformed (Coppetti et al. 2017) or distorted epidemiological records may arise.

Some individuals or population subgroups can also face inequalities in access to and use of mHealth. These can include individuals who have not been advised regarding the use of mHealth, who do not have a smartphone or access to internet or other relevant mHealth technology, do not know how to use mHealth technology, do not want to use it or do not use it for reasons of cost or battery capacity (Firth et al 2016, Malvey & Slovensky 2017). Others can be left behind or neglected by mHealth technologies that are not designed for diverse populations (AI NOW 2018).

Other considerations of justice are rarely discussed in the scholarly literature but they are highly relevant in our view. These include the tensions between social determinants of health (Marmot & Wilkinson 2006) and the resulting social gradient on the one hand and the emphasis on self-responsibility for health and healthy behaviour on the other (Voigt 2013; Wikler 2002). As discussed above, mHealth strongly encourages a shift towards self-responsibility for health, which is also supported by and even driven by economic interests, e.g. in the private IT and marketing sectors. Health insurance funds and private companies are increasingly using digital technologies to reward successful behavioural change or personal responsibility (AOK 2018; Barlyn 2018; Barmer, 2018). However, not everyone has the same living and working conditions that would enable them to make free, informed and well-balanced decisions in relation to their health (Voigt 2010). The shift towards self-responsibility could therefore lead to problematic finger pointing, especially towards the socially disadvantaged, and have serious implications for social values such as solidarity and social justice in health (Lupton 2016a).

ADVANCING MHEALTH WHILE UPHOLDING VALUES?

We have only briefly looked at a few aspects of mHealth here, but hope to have provided a glimpse into how profound the implications are for individuals and societies at large. mHealth technology is a tool that not only operates in the realm of health and well-being but that can also influence socio-politically relevant factors, such as knowledge production and social epistemology, and even democratic structures, economic interests and power patterns.

One area that has not been covered so far in this chapter pertains to the global implications of mHealth. Expectations are high that mHealth will be a crucial tool in reaching once difficult-to-reach populations, especially in remote communities in low- and middle-income countries (WHO 2011). It remains to be seen whether and how global health equity can be achieved through technology and which new ethical, legal and social implications will need to be discussed. For instance, can and should concepts of informed consent and data protection information be implemented and used universally? What are the implications of globally interacting IT companies and globally forming new patient collectives being connected through social media independent of national borders?

Altogether, unprecedented interest and power is being brought to bear by the IT and data sector, the private sector (including marketing) and users connecting on social media. The traditional boundaries of the health sector and expert knowledge are increasingly being blurred, if not left behind altogether. We are facing a "jumble" of overwhelmingly complex issues that overlap in ambiguous, contradictory and multi-dimensional ways. Implications on a societal and global level, which we are only beginning to unpack, are potentially dramatic. How should an analysis and interpretation of the implications of mHealth be undertaken and which values and norms should guide the various steps in relation to the technologies' development, dissemination and use?

Bioethics and public health ethics have analysed emerging health technologies for decades and should be well placed to investigate the normative implications of mHealth, especially in an interdisciplinary ELSA format. However, these disciplines are limited in terms of their methods and frameworks. As mHealth transcends and blurs the boundaries between traditional fields of health and medicine as well as the national boundaries of health systems, traditional research and analytical approaches have to be questioned and adapted. What is needed is an even more interdisciplinary, dynamic, flexible and creative approach to research questions and methods and a curiosity and openness towards technological innovation and the involvement of new stakeholders in the field of health and medicine, e.g. the globally operating private IT sector.

Given the complex implications beyond areas of health and medicine, analyses and interpretations of the implications of mHealth will inevitably go beyond traditional frameworks of bioethics and public health ethics. For example, issues of feminist concerns; sociological inquiries into disadvantage and power; relevant insights from social epistemology and political philosophy; and norms and paradigms in economics, globalisation and technology will have to be investigated more prominently.

Of central concern is finding the appropriate balance between the laudable effects on health itself and empowerment, democratisation and procedural improvements in health and healthcare, while limiting potentially negative developments so that ethical values can be upheld. Exploring and applying values such as justice, wellbeing, human rights, freedom, democracy, solidarity and diversity should guide the way towards good policy

and practice. At the same time, a generalised evaluation of mHealth is challenging, as each type of technology, and potentially even individual apps or sensors, might carry specific concerns, calling for a case-by-case analysis.

A digital health ethics that has a global scope but is yet informed by the socio-political specifics and needs of particular local contexts might be necessary. The ethics ought to understand, incorporate and address the above-mentioned shifts and transformations.

The overall aim of this piece, and ultimately of our larger research project "META", is to support responsible, socially and globally sustainable and user-centric innovation in mHealth. With this brief discussion of the complex ethical, legal and social dimensions of mHealth on individual, population and global levels and their implications, we hope to have contributed towards achieving this aim.

BIBLIOGRAPHY

Agarwal, D. K., Viers, B. R., Rivera, M. E., Nienow, D. A., Frank, I., Tollefson, M. K., & Gettman, M. T. (2018). Physical activity monitors can be successfully implemented to assess perioperative activity in urologic surgery. *MHealth, 4,* 43–43. https://doi.org/10.21037/mhealth.2018.09.05

AI NOW. (2018). *Algorithmic Accountability Policy Toolkit.* Retrieved from https://ainowinstitute.org/aap-toolkit.pdf

AOK. (2018). *Das AOK PLUS-Bonusprogramm - Gesundes Leben wird bei der AOK PLUS belohnt!* Retrieved from https://www.aok.de/pk/plus/inhalt/bonusprogramm/

Barlyn. (2018). *Strap on the Fitbit: John Hancock to sell only interactive life insurance.* Retrieved from https://www.reuters.com/article/us-manulife-financi-john-hancock-lifeins/strap-on-the-fitbit-john-hancock-to-sell-only-interactive-life-insurance-idUSKCN-1LZ1WL

Barmer. (2018). *Digital punkten mit der BARMER Bonus-App.* Retrieved from https://www.barmer.de/meine-barmer/online-services/bonusprogramm/digital-punkten-mit-der-barmer-bonus-app-164906

Bellekens, X., Hamilton, A., Seeam, P., Nieradzinska, K., Franssen, Q., & Seeam, A. (2016). Pervasive eHealth services a security and privacy risk awareness survey. *2016 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA)*, 1–4. https://doi.org/10.1109/CyberSA.2016.7503293

Borsari, L., Stancanelli, G., Guarenti, L., Grandi, T., Leotta, S., Barcellini, L., … Benski, A. C. (2018). An Innovative Mobile Health System to Improve and Standardize Antenatal Care Among Underserved Communities: A Feasibility Study in an Italian Hosting Center for Asylum Seekers. *Journal of Immigrant and Minority Health, 20*(5), 1128–1136. https://doi.org/10.1007/s10903-017-0669-2

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

Brownstein, J. S., Freifeld, C. C., & Madoff, L. C. (2009). Digital Disease Detection — Harnessing the Web for Public Health Surveillance. *New England Journal of Medicine, 360*(21), 2153–2157. https://doi.org/10.1056/NEJMp0900702

Chang, R. M., Kauffman, R. J., & Kwon, Y. (2014). Understanding the paradigm shift to computational social science in the presence of big data. *Decision Support Systems, 63,* 67–80. https://doi.org/10.1016/j.dss.2013.08.008

Coppetti, T., Brauchlin, A., Müggler, S., Attinger-Toller, A., Templin, C., Schönrath, F., … Wyss, C. A. (2017). Accuracy of smartphone apps for heart rate measurement. *European Journal of Preventive Cardiology, 24*(12), 1287–1293. https://doi.org/10.1177/2047487317702044

Eubanks, V. (2018). *Automating Inequality*. New York, NY: Saint Martin's Press Inc.

European Commission. (2014). Green Paper on mobile health ('mHealth'). Retrieved 14 June 2018, from Digital Single Market website: https://ec.europa.eu/digital-single-market/en/news/green-paper-mobile-health-mhealth

European Commission. (2018, April 25). *Communication on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society.* Retrieved from https://ec.europa.eu/digital-single-market/en/news/communication-enabling-digital-transformation-health-and-care-digital-single-market-empowering

Eysenbach, G. (2000). Towards ethical guidelines for e-health: JMIR Theme Issue on eHealth Ethics. *Journal of Medical Internet Research, 2*(1). https://doi.org/10.2196/jmir.2.1.e7

Fangerau, H., Griemmert, M., Albrecht, U.-V. (2016): Kapitel 9 - Gesundheits-Apps und Ethik, Chapter 9 – Health Apps and Ethics. In Albrecht, U-V. (Hrsg.) Chancen und Risiken von Gesundheits-Apps (CHARISMHA). p. 194-213.

Figueiredo, M., Caldeira, C., Chen, Y., & Zheng, K. (2017). *Routine self-tracking of health: reasons, facilitating factors, and the potential impact on health management practices*. 9.

Firth, J., Cotter, J., Torous, J., Bucci, S., Firth, J. A., & Yung, A. R. (2016). Mobile Phone Ownership and Endorsement of 'mHealth' Among People With Psychosis: A Meta-analysis of Cross-sectional Studies. *Schizophrenia Bulletin, 42*(2), 448–455. https://doi.org/10.1093/schbul/sbv132

Fornace, K. M., Surendra, H., Abidin, T. R., Reyes, R., Macalinao, M. L. M., Stresman, G., … Cook, J. (2018). Use of mobile technology-based participatory mapping approaches to geolocate health facility attendees for disease surveillance in low resource settings. *International Journal of Health Geographics, 17*(1). https://doi.org/10.1186/s12942-018-0141-0

Griauzde, D., Kullgren, J. T., Liestenfeltz, B., Ansari, T., Johnson, E. H., Fedewa, A., … Heisler, M. (2019). A Mobile Phone-Based Program to Promote Healthy Behaviors Among Adults With Prediabetes Who Declined Participation in Free Diabetes Prevention Programs: Mixed-Methods Pilot Randomized Controlled Trial. *JMIR MHealth and UHealth, 7*(1), e11267. https://doi.org/10.2196/11267

Hendl, T., Jansky, B. & Wild, V. (2019). From Design to Data Handling. Why mHealth Needs a Feminist Perspective. In Loh J. & Coeckelbergh M. (Eds.). *Feminist Philosophy of Technology.* Stuttgart: J.B.Metzler.

Khera, M. (2017). Think Like a Hacker: Insights on the Latest Attack Vectors (and Security Controls) for Medical Device Applications. *Journal of Diabetes Science and Technology, 11*(2), 207–212. https://doi.org/10.1177/1932296816677576

Kingod, N. (2018). The tinkering m-patient: Co-constructing knowledge on how to live with type 1 diabetes through Facebook searching and sharing and offline tinkering with self-care. *Health*, 1363459318800140. https://doi.org/10.1177/1363459318800140

Kitchin, R. (2014). Big Data, new epistemologies and paradigm shifts. *Big Data & Society, 1*(1), 2053951714528481. https://doi.org/10.1177/2053951714528481

Kluge, E.-H. W. (2017). Health Information Professionals in a Global eHealth World: Ethical and legal arguments for the international certification and accreditation of health information professionals. *International Journal of Medical Informatics, 97*, 261–265. https://doi.org/10.1016/j.ijmedinf.2016.10.020

Kotz, D. (2011). A threat taxonomy for mHealth privacy. *Third International Conference on Communication Systems and Networks (COMSNETS 2011)*.

Kreitmair, K., Cho, M., & Magnus, D. (2017). Wearable and mobile health technology: Consent and engagement, security, and authentic living. *NATURE BIOTECHNOLOGY, 35*(7). Retrieved from http://www.nature.com/articles/nbt.3887.pdf

Kreps, G. L., & Neuhauser, L. (2010). New directions in eHealth communication: Opportunities and challenges. *Patient Education and Counseling, 78*(3), 329–336. https://doi.org/10.1016/j.pec.2010.01.013

Lewis, D., & Leibrand, S. (2016). Real-World Use of Open Source Artificial Pancreas Systems. *Journal of Diabetes Science and Technology, 10*(6), 1411–1411. https://doi.org/10.1177/1932296816665635

Lupton, D. (2015a). Quantified sex: a critical analysis of sexual and reproductive self-tracking using apps. *Culture, Health & Sexuality, 17*(4), 440–453. https://doi.org/10.1080/13691058.2014.920528

Lupton, D. (2015b). Health promotion in the digital era: a critical commentary. *Health Promotion International, 30*(1), 174–183. https://doi.org/10.1093/heapro/dau091

Malvey, D. M., & Slovensky, D. J. (2017). Global mHealth policy arena: status check and future directions. *MHealth*, 3, 41–41. https://doi.org/10.21037/mhealth.2017.09.03

Marmot, M., & Wilkinson, R. G. (2006). *Social Determinants of Health.* OUP Oxford.

Mayer-Schönberger, V., & Cukier, K. (2013). *Big Data: Die Revolution, die unser Leben verändern wird.* München: Redline Verlag.

Nissenbaum, H., & Patterson, H. (2016). Biosensing in Context: Health Privacy in a Connected World. In *Quantified: Biosensing Technologies in everyday life* (pp. 79–100). Cambridge & London: MIT Press.

O'Neil, C. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (Reprint). Broadway Books.

Ospina-Pinillos, L., Davenport, T. A., Ricci, C. S., Milton, A. C., Scott, E. M., & Hickie, I. B. (2018). Developing a Mental Health eClinic to Improve Access to and Quality of Mental Health Care for Young People: Using Participatory Design as Research Methodologies. *Journal of Medical Internet Research, 20*(5), e188. https://doi.org/10.2196/jmir.9716

PwC. (2013). Socio-economic impact of mHealth: An assessment report for the European Union. *PricewaterhouseCoopers*. Retrieved from https://www.pwc.in/assets/pdfs/consulting/strategy/socio-economic-impact-of-mhealth-the-european-union.pdf

Rönkkö, K. (2018). An Activity Tracker and Its Accompanying App as a Motivator for Increased Exercise and Better Sleeping Habits for Youths in Need of Social Care: Field Study. *JMIR MHealth and UHealth, 6*(12), e193. https://doi.org/10.2196/mhealth.9286

Ruckenstein, M., & Schüll, N. D. (2017). The Datafication of Health. *Annual Review of Anthropology, 46*(1), 261–278. https://doi.org/10.1146/annurev-anthro-102116-041244

Sharon, T. (2017). Self-Tracking for Health and the Quantified Self: Re-Articulating Autonomy, Solidarity, and Authenticity in an Age of Personalized Healthcare. *Philosophy & Technology, 30*(1), 93–121. https://doi.org/10.1007/s13347-016-0215-5

Sharon, T., & Zandbergen, D. (2017). From data fetishism to quantifying selves: Self-tracking practices and the other values of data. *New Media & Society, 19*(11), 1695–1709. https://doi.org/10.1177/1461444816636090

Steinhubl, S. R., Muse, E. D., & Topol, E. J. (2015). The emerging field of mobile health. Sci Transl Med, 7(283), 1–12. https://doi.org/10.1126/scitranslmed.aaa3487

Swan, M. (2012). Health 2050: The Realization of Personalized Medicine through Crowdsourcing, the Quantified Self, and the Participatory Biocitizen. *Journal of Personalized Medicine, 2*(3), 93–118. https://doi.org/10.3390/jpm2030093

Tierney, W. G., Corwin, Z. B., & Ochsner, A. (2018). *Diversifying Digital Learning: Online Literacy and Educational Opportunity.* JHU Press.

Uthman, O. A., Nduka, C. U., Abba, M., Enriquez, R., Nordenstedt, H., Nalugoda, F., … Ekström, A. M. (2019). Comparison of mHealth and Face-to-Face Interventions for Smoking Cessation Among People Living With HIV: Meta-Analysis. *JMIR MHealth and UHealth, 7*(1), e203. https://doi.org/10.2196/mhealth.9329

Voigt, K. (2010). Smoking and Social Justice. *Public Health Ethics, 3*(2), 91–106. https://doi.org/10.1093/phe/phq006

Voigt, Kristin. (2013). Appeals to individual responsibility for health--reconsidering the luck egalitarian perspective. *Cambridge Quarterly of Healthcare Ethics: CQ: The International Journal of Healthcare Ethics Committees, 22*(2), 146–158. https://doi.org/10.1017/S0963180112000527

WHO. (2011). *mHealth: new horizons for health through mobile technologies: second global survey on eHealth.* Retrieved from http://apps.who.int/iris/handle/10665/44607

Wiederhold, B. K. (2012). Self-Tracking: Better Medicine Through Pattern Recognition. *Cyberpsychology, Behavior, and Social Networking, 15*(5), 235–236. https://doi.org/10.1089/cyber.2012.1545

Wikler, D. (2002). Personal and social responsibility for health. *Ethics & International Affairs, 16*(2), 47–55.

Plurality of values in mHealth: Conventions and ethical dilemmas

VALESKA CAPPEL AND KAROLIN EVA KAPPLER

The pragmatic economics of conventions offers new insights into mHealth, providing a deeper understanding of current ethical problems.

Keywords: economics of conventions, mHealth, plurality of values, materialities, ethical dilemma

THEORETICAL INTRODUCTION TO THE ECONOMICS OF CONVENTION IN THE FIELD OF (M)HEALTH

By conducting a pragmatic analysis of digitisation and mHealth, we want to introduce a new fundamental perspective to shed light on the moral and ethical questions arising from mHealth.

As a general social science theory, the economics of conventions (EC) offers consistent pragmatic concepts for the sociological analysis of social institutions, social cognition, social actions, social interactions and coordination processes, social constructions of facts, and social entities and their qualities. EC conceives of conventions as deeper and more general logics of coordination, interpretation and evaluation that actors apply in situations (Diaz-Bone 2018). From this perspective, actions are always the result of a process (Eymard-Duvernay et al. 2011) and are characterised by coordination between individuals and their social and material environments (Diaz-Bone 2018). Therefore, and in addition to the actors, conventions (Boltanski & Thévenot 2007), forms and objects (Thévenot 1984, 2001) become relevant by partly defining the meaning and social relevance of health. Adopting this theoretical perspective, we focus on health as a category that has to be mobilised in the first place (Foucault 1973; Ewald 1993) and has to be seen as a plural social institution (Collyer 2015; Batifoulier, Da Silva & Domin 2018; Da Silva 2018) that is enforced by ongoing digital transformations (Ruckenstein & Dow Schüll, 2017; Sharon 2018). Related to the EC perspective, we assume that the implementation of mHealth is guided by a plurality of logics, which causes – at least partially – (ethical) conflicts among them.

Research on health from an EC perspective illustrates this plurality of logics in different health-related fields. Regarding physicians' private practices, research has shown a shift from an inspired/domestic convention to an industrial convention, with strong implications for commodification, deliberation and rationalisation (Da Silva 2018; Batouflier

DOI: 10.5281/zenodo.3296885

et al. 2018).[1] Further, research indicates that social security is not always understood as a consciously established welfare-state institution but rather as the result of three competing conventions: an anti-capitalist one, a solidary one, and a liberal one. These three conventions are used by the involved actors to justify decisions to criticise existing policies in the welfare state. Consequently, welfare-state institutions can be understood as a specific result of these negotiations (Batifoulier, Da Silva & Vahabi 2019). Further, Sharon (2018) applies EC to the "googlisation of health research", which enlarges the dichotomy between public benefit and private, corporate gain in health research. She depicts five moral repertoires that draw upon different conceptualisations of the common good, as shown in Table 1 (cells without grey shading).

We expand Sharon's analysis to the field of mHealth, focusing on the conventions inscribed into mHealth technologies. As part of this, we examine some published fact-sheets[2] and guidelines[3] of the public eHealth agency eHealth Suisse. Competence and Coordination Office of the Confederation and the Cantons. This agency is intended to support and guide developers, users and legislators in the field of mHealth, in particular with the introduction of electronic patient files. We also combine these results with findings of the DFG-funded project "Taxonomies of the self. Emergence and social generalisation of calculative practices in the field of self-inspection", which examined health and fitness tracking and the emergence of new taxonomies based on interviews with self-tracking individuals.

PRELIMINARY EMPIRICAL RESULTS: CONFLICTING MORAL REPERTOIRES PRESENTED IN MHEALTH

Preliminary results show that the eHealth agency publications perceive three main problems or difficulties in the adoption of mHealth: first, data protection and data security, second, the standardisation of data technology (interoperationality) and, third, the intended and actual use of mHealth technologies.

To begin with the first of these problems, data security evokes different conventions. On the one hand, the domestic convention problematises the fact that users of mHealth technologies must strongly trust in data security as a precondition for sharing their sen-

[1] For more information about the different conventions, please see Diaz-Bone 2018.

[2] eHealth Suisse (2010): Der Nutzen von eHealth; eHealth Suisse (2010): OID-Konzept für das Schweizerische Gesundheitswesen; eHealth Suisse (2012): Zertifizierung der Qualität von Gesundheitsinformationen im Web; eHealth Suisse (2014): Nutzen des elektronischen Patientendossiers aus Sicht der Patienten; eHealth Suisse (2014): Nutzungsmöglichkeiten von SNOMED CT in der Schweiz; eHealth Suisse (2014): Studienresultate zum Thema „eHealth" und elektronisches Patientendossier.

[3] Study by order of eHealth Suisse: Endl et al. (2015): "mHealth im Kontext des elektronischen Patientendossiers. Eine Studie im Auftrag von eHealth Suisse".

sitive health data with selected interest groups. On the other hand, and following the logic of the civic convention, data protection must be formally guaranteed for reasons of transparency and liability; this may occur via official certification mechanisms.

As far as the second issue is concerned, the absence of standardisation in the area of mHealth is problematised by different conventions for various reasons: standardising the many different devices and applications to meet the technical requirements of the electronic patient dossier is viewed as a challenge. From the perspective of an industrial convention, standardisation allows the planning, efficiency, functionality and competence of mHealth technologies and with it the possibility to develop quality standards for health information and acceptance. The civic convention also advocates standardisation to ensure the quality and credibility of digital medical information for all citizens. In contrast, and from the perspective of the market convention, standardisation is necessary for monetary reasons, for instance, for insurers to reimburse services related to mHealth technologies or to divide the costs and benefits of mHealth between different stakeholders.

Third, the lack of a widespread use of mHealth-technologies is also problematised from the perspective of several conventions. From the perspective of the vitality convention, a broad use of mHealth technologies should prompt people to deal with their health and thus remain healthier. Ideally, mHealth technologies should be more person-centred than previous treatment processes. From a civic convention perspective, the question of whether the introduction and application of mHealth technologies is wanted and accepted by the population is an issue.

As long as different conventions pursue the same goal for different reasons, no conflicts are expected. Nevertheless, and considering the three mentioned problems – data protection, standardisation and use of mHealth technologies – some lines of conflict seem to appear between them. The broad use of mHealth technologies seems to be linked to trust in high data security (domestic and civic convention) and high quality standards through certification (industrial convention). From the perspective of an industrial convention, the successful implementation of mHealth technologies depends on the integration of private providers, which mainly follow market conventions due to the lucrative mHealth market. Furthermore, this could lead to a conflict between the industrial/market conventions, both of which favour the integration of private providers, and the domestic and civic conventions. This is because both private insurance companies and private manufacturers of wellness and fitness mHealth apps need to collect, share and evaluate data to successfully implement their business model. Another conflict can be expected to arise between standardisation and the idea of improving individual health. Standardisation complicates the individual relationship between doctor and patient and cannot really capture the individual reality of life, which often follows an inspired and industrial or domestic logic. Hence, and as shown in our interviews with mHealth users in the DFG project, they seem to accept and tolerate the industrial convention only up to

a certain point. Therefore, they transform the numbers, averages and comparisons into qualified data (Swan 2013), following an inspired/domestic convention. Analysing the users' perspective and practices, we find evidence of a continuum that spans a quantifying, goal-oriented approach according to an industrial logic and a curious-explorative and above all self-focused approach following an inspired logic, although even the practices that appear to be planned and objective are placed in a logic of intrinsically motivated self-care.

Consequently, our analysis extends Sharon's table on moral repertoires by adding two more conventions: the domestic and the inspired one (see Table 1). Further, our results depict some current and forthcoming conflicts, mainly emerging between the industrial/market conventions and the domestic/inspired logics as well as the civic logic.

PLURALITY OF VALUES IN MHEALTH AND THEIR CONSEQUENCES FOR ETHICAL DECISIONS

The EC perspective shows that mHealth technologies are also technical objects that suggest an instrumental relationship to nature and thus a kind of objectivity. But to measure health, it is necessary to determine what should be measured, how it should be measured and for what purpose. When considering a technical object, like a health app, one might assume it measures a natural state. But there is no universal "natural" state of health that could be measured without a context. The interests and values that lead to the measurement of specific health parameters (see Table 1) can quickly become invisible through the technical object (Boltanski & Thévenot 2007). Actors are guided by conventions in all situations, also when defining, measuring and implementing health. With this orientation, they link their evaluation and critique of digital data and "digital health", either by planning to measure health or by judging the results of the measurements.

For mHealth applications, this means developing a health plan that fits numbers, signs and codes. So, there is a need for a digital representation of health. This leads – from an ethical perspective – to the following question: how could and should this work? What logic of a common good legitimises decisions and how could and would we decide if we were able to discuss the different logics represented in Table 1? The evaluation and acceptance of digital applications can only be understood when the plurality of these value logics is considered and consulted. Different and conflicting "logics of values" may result in criticism or rejection of mHealth technologies, as shown in the conflict that arises when mHealth users expect a domestic or inspired logic, while the technology incorporates an industrial one.

TABLE 1: MORAL REPERTOIRES PRESENT IN MHEALTH (SHARON 2018 AND OWN ELABORATION (IN GREY))

Repertoire	Common good	Values	Example (translations by authors)	mHealth(care) as
Civic	Collective well-being	Inclusivity, solidarity, equality	"Provide reliable guidance"	A human righ
Market	Economic growth	Competition, consumer choice, profit	"The evaluation and establishment of standards and norms is therefore one very important condition for the dissemination and economic use of mHealth."	A market good
Industrial	Increased efficiency	Functionality, expertise, optimisation	"the greatest benefit lies in the exchangeability of data, so in interoperability"	A (data) system to streamline
Project	Innovation and the network	Activity, experimentation, connection	"mHealth services offer great potential, the collection of huge amounts of health data (Big Data) to facilitate them. These data enable research and innovation continues to advance in the field of health care"	A project requiring innovation
Vitality	Greater health	Good health, life, vitality	"...contributes to the responsible use of one's own health and thus helps to increase health literacy"	Intrinsically worthy
Domestic	Tradition	Hierarchy, trust	"…so I developed a good sense of when my pulse goes up. So actually I know what's on the clock "	Socialised/ learned health knowledge
Inspired	Inspiration and deliberation	Spontaneity, emotion, creativity	"We are not average people but everyone is an individual. For an individual, other rules count"	A result of body and soul-experience

CONCLUSION

The different valuation logics can lead - in an institutionalised context, e.g. in medical examinations or insurance agreements – to permanent conflicts, such as the rejection of mHealth applications. EC can help identify potential lines of conflict in the implementation of mHealth at an early stage, recognising the plurality of (moral) values in specific situations. It is crucial that this plurality of moral orders is taken seriously, as these orders influence decision-making, actions, technology development and usage. Thus, EC can contribute to the detection, description and resolution of ethical dilemmas.

BIBLIOGRAPHY

Batifoulier, P., Braddock, L. & Latsis, J. (2013). Priority setting in health care: from arbitrariness to societal values. *Journal of Institutional Economics, 9*(1), 61–80.

Batifoulier, P., Da Silva, N. & Domin, J.-P. (2018). Economie de la santé. Paris: Armand Colin.

Batifoulier, P., Da Silva, N. & Vahabi, M. (2019). A theory of predatory welfare state and citizen welfare: the French case. *CEPN Working Papers,* No 2019-03. Paris: University of Paris 13.

Boltanski, L. & Thévenot, L. (2007). *Über die Rechtfertigung. Eine Soziologie der kritischen Urteilskraft.* Hamburg: Hamburger Edition.

Collyer, F. (2015). *The palgrave handbook of social theory in health, illness and medicine.* London: Palgrave Macmillan.

Da Silva, N. (2018). L`Industrialisation de la médicine libérale. Une approche par l'économie des conventiones. *Management & Avenir Santé. L'industrialisation de la santé, 1*(3), 13-30.

Diaz-Bone, R. (2018). *Die "Economie des conventions". Grundlagen und Entwicklungen der neuen französischen Wirtschaftssoziologie* (2nd. ed.). Wiesbaden: Springer VS.

Ewald, F. (1993). *Der Vorsorgestaat.* Frankfurt: Suhrkamp.

Eymard-Duvernay, F., Favereau, O., Salais, R., Thévenot, L. & Orléan, A. (2011). Werte, Koordination und Rationalität: Die Verbindung dreier Themen durch die "Économie des conventions". In R. Diaz-Bone (Ed.), *Soziologie der Konventionen. Grundlagen einer pragmatischen Anthropologie* (pp. 203-230). Frankfurt: Campus.

Foucault, M. (1973). *Die Geburt der Klinik. Eine Archäologie des ärztlichen Blicks.* München: Carl Hanser Verlag.

Ruckenstein, M. & Dow Schüll, N. (2017). The Datafication of Health. *Annual Review of Anthropology,* 46, 261-278.

Sharon, T. (2018). When digital health meets digital capitalism, how many common goods are at stake? *Big Data & Society,* July-December: 1-12. doi: 10.1177/2053951718819032

Swan, M. (2013). The Quantified Self: Fundamental Disruption in Big Data Science and Biological Discovery. *Big Data, 1*(2).

Thévenot, L. (1984). Rules and implements: Investments in forms. *Social Science Information, 23*(1), 1-45.

Thévenot, L. (2001). Organized complexity. Conventions of coordination and the composition of economic arrangements. *European Journal of Social Theory, 4*(4), 405-425.

Processing purposes

TRIX MULDER

INTRODUCTION

The healthcare sector has traditionally processed large amounts of personal data. The rise of information technologies, such as smartphone applications ("apps") and wearable devices (e.g. Fitbit, smart soles) both inside and outside medical practice, has added to the processing of these kinds of personal data. Commercial apps and wearables that aim to encourage health behaviour change are flourishing in the major app stores. These technologies enable people to monitor their own health by using (pressure) sensing technologies that measure vital signs (for example, heartrate) and track progress (such as counting steps), without having to visit a doctor.[1] A new complicating factor is that these so-called commercial health apps and wearables are increasingly being used within a medical context. The data generated transcends the closed context of personal medical records, geographic borders and, in particular, the borders of the European Union. This is problematic, because no current regulations address the global dimension of data.[2]

Legislative bodies worldwide have tried to deal with this global dimension of data, and if 2018 proved one thing, it is that legal data protection is very much alive and kicking.[3] Both the European Union and the Council of Europe, the two major European legislators, updated their legal instruments relating to data protection, which originated from the last century. The Council of Europe updated their Convention 108[4] and the General Data Protection Regulation (GDPR)[5] entered into force on 25 May 2018. Outside the European Union, the State of California followed this trend with the California Consumer Privacy Act 2018 (CCPA)[6] on 29 June 2018. The CCPA will enter into force on 1 January 2020. These legal changes are required, since information technologies are evolving quickly and regulation is trying to keep up to avoid a growing gap.[7]

[1] Brad Millington, 'Smartphone Apps and the Mobile Privatization of Health and Fitness' (2014) 31:5 Critical Studies in Media Communication 479.

[2] Denis Kelleher, EU Data Protection Law (Bloomsbury Publishing Plc 2018) 109.

[3] Graham Greenleaf, ''Modernised' Data Protection Convention 108 and the GDPR' (2018) 154 Privacy Laws & Business International Report 22 < http://www.ssrn.com/link/UNSW-LEG.html > accessed 10 May 2019.

[4] Convention for the protection of individuals with regard to automatic processing of personal data [1981] ETS No. 108 (CM/Inf (2018) 15-final).

[5] European Parliament and Council Regulation (EU) 2016/679 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) [2016] OJ L 119/1.

[6] California Consumer Privacy Act (CCPA) AB 375.

[7] Andrew Askland, 'Introduction: Why Law and Ethics Need to Keep Pace with Emerging Technologies' in Gary Marchant, Braden Allenby and Joseph Herkert (eds), The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight (Springer 2011) xiii.

DOI: 10.5281/zenodo.3296915

LEGAL CHALLENGES

The use of these commercial health apps within medical practice creates several legal challenges, such as reconciling these apps with data protection laws and principles. This is especially relevant because the two major legal frameworks that regulate data protection in Europe characterise these kinds of personal data as a special category of data, also referred to as sensitive data.[8] These data protection regulations also determine that personal data can only be processed for specific, explicit and legitimate purposes.[9] This is referred to as purpose limitation. The Draft Code of Conduct on privacy for mobile health applications also acknowledges this principle.[10] This research offers an analysis of the principle of purpose limitation in European data protection law and examines how the privacy policies of health apps deal with this principle in practice so that legal obstacles to using commercial health apps in a medical practice can be revealed. Furthermore, it will discuss lawful ways to handle such obstacles. This could increase adoption of commercial apps in clinical practice and affect the development of the next generation of health apps.

MODERN TECHNOLOGIES

Well over 320,000 health apps[11] are available on the major app stores (Apple, Google and Microsoft). For example, Fitbit has over 25 million active users worldwide, the Nike app registers over 1.8 million workouts per month worldwide and 8 million activities are uploaded on the Strava app every day, worldwide. This shows that health apps are an important part of our global society. However, global regulation on data protection is lacking.[12] Furthermore, it is not always clear how the companies that offer these eHealth technologies and services protect the health data they generate. It is thus not surprising that the digital transformation of health and care has become a priority EU issue. See for example, the communication on enabling the digital transformation of health and care in the digital single market, empowering citizens and building a healthier society.[13]

Because of the large number of different health apps in the three major app stores (Apple, Google and Windows/Microsoft), investigating all these apps would go beyond the scope of this exploratory research. This research offers purely theoretical observa-

[8] Article 9 GDPR and Article 6 Modernised Convention 108.

[9] Article 5 (1,c) GDPR and Article 5 (4,b) Modernised Convention 108.

[10] Draft Code of Conduct on privacy for mobile health applications < https://ec.europa.eu/digital-single-market/en/news/code-conduct-privacy-mhealth-apps-has-been-finalised > accessed 13 May 2019, 7.

[11] Sometimes literature uses the term "lifestyle apps" or "wellbeing apps" to describe apps that aim health behaviour change. In this paper, I chose to use the term "health apps" to refer to these apps.

[12] Kelleher (n 1) 109.

[13] Brussels COM 2018, 233 final.

tions on the question whether the purposes used in the analysed privacy policies match the purposes used by the healthcare sector.[14] Three local rehabilitation centres in the Netherlands showed interest in this research and offered their cooperation.[15] Via a short questionnaire, physicians in these three rehabilitation centres were asked three questions about apps they already use, apps they want to use and apps patients suggested using.[16] In total, 34 different apps were mentioned by at least one physician. These apps were selected for this research. At the end of the research period, four apps were no longer available, which left this research with thirty apps.

PURPOSE LIMITATION IN EUROPEAN PRIVACY LAWS

The GDPR and modernised Convention 108 determine that purpose limitation is one of the general principles relating to the processing of personal data. It means that personal data can only be collected for specified, explicit and legitimate purposes and cannot be processed further in a manner that is incompatible with the original purposes for processing.[17] Since purpose limitation is a general principle, it applies both to the processing of sensitive data and other (non-sensitive) personal data. Both the Council of Europe and the European Union have deemed purpose limitation a "key principle and stable element" regarding data protection legislation for years.[18]

Due to the principle of purpose limitation, personal data cannot be processed for other purposes than the purpose for which the personal data was originally intended. If someone wants to process the personal data for another purpose, the data subject's consent is needed in most cases.[19] In the case of sensitive data, regular consent is not enough. Either explicit consent is needed[20] or appropriate safeguards have to be enshrined in law.[21]

The GDPR offers guidelines for controllers by pointing out five elements controllers have to take into account to help determine whether processing for another purpose is

[14] Robert Yin, Case Study Research, Design and Methods (5th edn, Sage Publications 2014) 40.

[15] Beatrixoord, Roessingh and De Hoogstraat.

[16] The questions were: 1. Do patients ever suggest using an app or wearable in their rehabilitation process that they already use or would like to use and, if so, which apps and wearables are this and where do they want to use them for? 2. Have you ever advised an app or wearable yourself and, if so, what apps or wearable and for what part of the rehabilitation process?; 3. Are there apps or wearables that you have not yet advised, but would like to advise and if so what would that app or wearable be suitable for?;
One of the revalidation centers conducted a similar inquiry themselves a few weeks earlier, therefore the data of those questionnaires where used instead of the questions above.

[17] Ibid (n 9).

[18] Nikolaus Forgó, Stefanie Hänold and Benjamin Schütze, 'The Principle of Purpose Limitation and Big Data' in Marcelo Corrales, Mark Fenwick and Nikolaus Forgó (eds), New Technology, Big Data and the Law (Springer 2017) 22.

[19] Article 6 (1,a) GDPR and Article 5 (2) Modernised Convention 108.

[20] Article 9 (2,a) GDRP.

[21] Article 6 (1) Modernised Convention 108.

compatible with the original purpose.[22] Although the list is not exhaustive, it does give the controller some guidance. First, the controller has to take into account "any link between the purposes for which the personal data have been collected and the purposes of the intended further processing".[23] Second, the "context in which the personal data have been collected, in particular regarding the relationship between data subject and the controller"[24] are important. Third, the "nature of the personal data, in particular whether special categories of personal data are processed"[25] has to be taken into account. Also, the "possible consequences of the intended further processing" for the data subject have to be considered. Finally, the "existence of appropriate safeguards",[26] including encryption or pseudonumisation, have to be taken into account.

Before any conclusions can be drawn on the question of whether or not the purposes for processing the personal data collected via commercial apps and wearables are compatible with the processing of that personal data in a medical context, the processing purposes of both have to be mapped out so they can be compared.

PURPOSES FOR PROCESSING PERSONAL DATA

This paragraph will describe the processing purposes of commercial health apps and wearables and those of the healthcare sector.

Healthcare sector

In the healthcare sector, there are several purposes for processing personal data from patients. The most important ones are to provide patient care and to support the administration of patient care. Processing is also necessary for billing and for submitting reimbursement claims to healthcare insurance companies.[27] In university medical centres, personal data might also be processed for research purposes.

In most cases, personal data collected via commercial health apps and wearables will be used in a patient treatment plan. Therefore, the purpose of processing these kinds of data will correlate with the first purpose: providing patient care. Data concerning health cannot be processed unless one of the exemptions mentioned in Article 9 (2) are met. For medical treatment, Article 9 (2,h in conjunction with 3) GDPR allows the processing of these kinds of data when these data are necessary for a medical diagnosis and they are being processed by or under the responsibility of someone who is subject to the

[22] Article 6 (4) GDPR.

[23] Ibid.

[24] Ibid.

[25] Ibid.

[26] Ibid

[27] For example: Processing of Patient Personal Data, a guideline for General Practitioners 2018.

obligation of professional secrecy. Although it could be argued that data collected via commercial health apps and wearables are necessary for a medical diagnosis, the data are not being processed by or under the responsibility of someone who is obliged to maintain professional secrecy. Therefore, the explicit consent of the data subject is needed.[28] Even though this could be arranged, there is another problem regarding the processing of these kinds of data in a medical context. This has to do with the way the processing purposes are described in the privacy policies of these commercial health apps and wearables.

Privacy policies and purposes

Commercial apps and wearables usually ask the user for consent to the processing of their personal data via privacy policies. Our investigation of several privacy policies of commercial health apps and wearables showed that the purposes for processing are typically quite vague. For this research, we analysed thirty privacy policies. The privacy policies do not use a standard format; therefore, we identified 19 different processing purposes, ranging from providing services to marketing and sharing with third parties. A complete overview of the purposes, with an example, can be found in Table 1.

As Table 1 shows, most of these purposes are explained in rather vague terms. The privacy policies mention, that the companies want to use the personal data to "improve and maintain products and services", without being clear on what part of the personal data are being used for this purpose and what "products and services" are meant. Other privacy policies mention that they process personal data, such as the "use of workout data". Although the privacy policy does mention that the nature of these data are "in some jurisdictions" considered to be sensitive data, the privacy policy does not elaborate on how these data are used. It only mentions that the company will "take appropriate measures in protecting and using this data and (…) will obtain consent before they use these kinds of data."

Although this is only a small selection of the vague processing purposes, it makes clear that most of these vague descriptions are not in accordance with the GDPR. After analysing thirty privacy policies, it was still very hard to determine the exact purposes for processing personal data and therefore it was not clear what the user had to consent to. The implication of this is as follows: if we do not take action, we will lose purpose limitation as a safeguard for data protection. After all, if we do not know what we are consenting to when we agree to privacy policies, this might affect the validity of our consent.

[28] Article 9 (2,a) GDPR.

TABLE 1: PURPOSES FOR PROCESSING PERSONAL DATA

Purpose	Example
Provide service	To improve and maintain products and services
Administer service	For customer support
Users experience	To personalise and improve your experience
Provide care	To provide care
Medical procedure /treatment	The most important place we store your data is in the Electronic Patient File
Declaration of healthcare costs	To declare healthcare costs (to insurers or the patient)
Information provision	For software updates, events, products
Dealing with complaints	We process your personal information when you contact us to help you with any questions, concerns, disputes or issues
Communication with user	To send the user service notifications and respond to the user
Qualitative goals	To enhance and improve application
Safety and security	For the safety and security of the services, users and other parties
Legal obligations	To fulfil legal obligations or to protect from legal claims
Research	To understand customer behaviour or preference
Marketing purposes	Advertise and market to users, which includes sending promotional communications, targeting advertising, and presenting you with relevant offers
Sales activities	Processing orders
Identity confirmation	We may use your personal data to confirm your identity
Management operations	Supporting operational management
Audits	We may also use your personal data for internal matters, such as audits and data analyses
Sharing with third parties	To help advertisers and other partners measure the effectiveness and distribution of their ads and services and their users

CONCLUSIONS

Although the privacy regulations implemented in Europe in 2018 determine that purpose limitation is a key concept in data protection, the privacy policies of commercial health apps do not comply with these rules. This is despite the fact that the Draft Code of Conduct on privacy for mHealth apps acknowledges purpose limitation as a key element in data protection, especially regarding data concerning health. Therefore, the use of these commercial apps and wearables in a medical context is difficult. This is particularly relevant because data protection laws in Europe categorise health data as sensitive data, which can, in principle, not be processed. Further cooperation between the European Data Protection Board (EDPB) and representatives of app providers and the healthcare sector on this matter is desirable, given that, together, they can create solutions that benefit all, including data subjects. This will make it easier for all app providers to comply with the GDPR and the modernised Convention 108, taking account of the particular needs of the healthcare sector, and it will support national supervisory authorities in enforcing these regulations.

BIBLIOGRAPHY

Askland A, 'Introduction: Why Law and Ethics Need to Keep Pace with Emerging Technologies' in Gary Marchant, Braden Allenby and Joseph Herkert (eds), *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight* (Springer 2011).

Brussels COM 2018, 233 final.

California Consumer Privacy Act (CCPA) AB 375.

Convention for the protection of individuals with regard to automatic processing of personal data [1981] ETS No. 108 (CM/Inf (2018) 15-final).

Draft Code of Conduct on privacy for mobile health applications <https://ec.europa.eu/digital-single-market/en/news/code-conduct-privacy-mhealth-apps-has-been-finalised>

European Parliament and Council Regulation (EU) 2016/679 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) [2016] OJ L 119/1.

Processing of Patient Personal Data, a Guideline for General Practitioners 2018.

Forgó N, Hänold S and Schütze B, 'The Principle of Purpose Limitation and Big Data' in Corrales M, Fenwick M and Forgó N (eds), *New Technology, Big Data and the Law* (Springer 2017).

Greenleaf G, ''Modernised' Data Protection Convention 108 and the GDPR' (2018) 154 Privacy Laws & Business International Report 22. http://www.ssrn.com/link/UNSW-LEG.html (accessed 10 May 2019).

Kelleher D, *EU Data Protection Law* (Bloomsbury Publishing Plc 2018).

Millington B, 'Smartphone Apps and the Mobile Privatization of Health and Fitness' (2014) 31:5 Critical Studies in Media Communication.

Yin R, *Case Study Research, Design and Methods* (5th edn, Sage Publications 2014).

On the ethical challenges of innovation in digital health

THOMAS CHRISTIAN BÄCHLE

The evaluation of technological innovation needs to take into account a multitude of different areas, each of which with unique ethical repercussions.

Keywords: autonomy, hybrid responsibility, overdiagnosis, predictive diagnostics, self-governance

INTRODUCTION

The relationship between innovation and ethics is ambiguous. On the one hand, ethical considerations are often said to be an obstacle to social or technological progress, constraining innovative approaches for the sake of being overly cautious. In that vein, codes of conduct, ethical review commissions or public debates on controversial topics such as genome editing might delay the implementation of technological solutions to pressing social and medical problems. On the other hand, while ethical principles reassuringly prevent an anything-goes attitude, they can even come to act as drivers of innovative approaches and even become a decisive factor in the competition for ideas. Of course, neither of these two contradictory viewpoints is valid on its own. Ethical considerations need to go hand in hand with innovation and should not be just an afterthought. It is a truism that any new technology poses a trade-off between benefits and risks. The advent of digital technologies, however, introduces challenges that concern all aspects of life but particularly the sensitive area of health, where a long tradition of ethical principles applies.

These "foundational ethical principles" include non-maleficence (effectively summed up in the famous dictum *primum non nocere*), beneficence (actions that are in a patient's best interest), the respect for a person's autonomy, and justice (in particular, an equal distribution of goods, services or resources); specifically in therapeutic contexts, they also include the principle of fidelity (trust comprising both loyalty and honesty) (Strohm Kitchener & Anderson 2011). When assessing medical and health-related innovations, these principles can be translated into a very general framework of questions that guide ethical concerns:

1. Is the innovative technology harmful? What are potential risks associated with it?
2. What are its potential benefits and is there evidence available to substantiate them?
3. How will this innovation affect the autonomy of affected parties?

DOI: 10.5281/zenodo.3296931

4. How will the innovation affect justice and equity? Will access to the innovative technology be equally distributed? Will it create new inequalities?
5. Which effect will the innovation have on the relationship between patient and physician, therapist or counsellor?

As will be seen in the discussion of the following four issues – the role of data and data analytics, responsibility, (over)diagnosis and autonomy – which are among the most important ethical challenges in the context of eHealth innovations, the answers to these questions are far from obvious.[1]

ANY DATA CAN BECOME "HEALTH-RELATED"

The *universal datafication* and subsequent analysis of large data sets ("big data") of medically relevant information (such as biochemical and genetic information) has been expanded to include physical, social and cultural factors that are creating an unprecedented level of knowledge about each individual. Data repositories maintained by large private companies such as Apple and Alphabet permeate the field of services related to health and well-being. When looking at the issue of data, it is by no means solely the large quantity of data sets that is highly consequential. Digital communications technologies not only allow for representations of all actions, behaviours and (communicative) interactions in minute detail. In addition, these very activities generate additional information that can also be used to accumulate data (Andrejevic 2007). This universal surveillance is based on "extractive processes" that "typically occur in the absence of dialogue or consent, despite the fact that they signal both facts and subjectivities of individual lives (Zuboff 2015, 79). This represents a type of capitalism that introduces "unexpected and often illegible mechanisms of extraction, commodification, and control that effectively exile persons from their own behavior while producing new markets of behavioral prediction and modification" (Zuboff 2015, 75). Based on intricate methods of data analysis used to determine significant patterns – often labelled "artificial intelligence" (AI) or machine learning – this means that any type of data can become *meaningful* in a health-related context, whether it is one's eating, sleeping and drinking habits, personal interests and social ties, or one's appearance or voice. In addition, machine learning analytics can potentially identify previously unknown patterns between variables and create new knowledge about individuals and group affiliations, such as "people who experienced X when they were 10 years old are likely to develop condition Y once they turn 40".

[1] Some of the arguments made in this text were represented in the discussion entitled "Ethics and Innovation" at the "Futures of eHealth" conference which took place on 30 April 2019 in Berlin. Participants were Btihaj Ajana (King's College London), Erwin Böttinger (Digital Health Center, Hasso-Plattner-Institute, Potsdam), Elif Kücüktas (chair), Daniel Strech (Berlin Institute of Health) and Jai Ganesh Udayasankaran (Asia eHealth Information Network).

The universal collection of personal data raises obvious issues such as data security and confidentiality but also entails much less visible consequences, such as a slow change in our understanding of what it means to be healthy and the general tendency to overdiagnose or overtreat. The collection of data is sometimes intentional (with self-tracking devices and lifestyle apps) but often happens inadvertently, with a smartphone being used as a universal tracking device. This raises the question of control of the potentially health-related data that is being collected, stored and analysed by large private companies. Although it is customers who buy and own a device and its materiality, the software, the application and most importantly the data thus generated is not held by them (Fairfield 2017).[2] This is particularly noteworthy, since the data is produced by each *individual's* actions and corporeal physicality but is monetised by third parties (Ajana 2017). "Paying off" people for the data they generate only offers a purely economic solution to an economic problem but will likely further deepen social divides, since it leads to an even stronger commercialisation of the data that may overlook social, legal or ethical perspectives (Prainsack 2017). This is also the case when the more affluent individuals, groups or populations are able to pay for any service they want while their data is kept private and secure. Creating a business model that is both viable and "ethical" and that factors in issues such as self-determination, responsibility and social power structures is still an unresolved challenge.

The health-related data that is generated via commercial self-tracking devices must be differentiated from the data that is collected, stored and processed in biomedical research contexts. From an ethical perspective, however, similar issues are concerned, namely informed consent, privacy (including anonymisation and data protection), control of personal data and the questionable objectivity of "big data" analyses (Mittelstadt/Floridi 2016). Ensuring informed consent in biomedical research promises transparency and even citizen empowerment, with people taking control of their own data. In reality, however, people often do not understand what they are consenting to. In the case of data and machine learning tools, this concerns diagnostics systems that – given their self-learning and automatic nature – have a future scope of knowledge (diagnostic, research or otherwise) that cannot be fully understood at present. Will and should the informed consent include these unknowns? How can this complexity be made transparent to patients and physicians in order to ensure informed decisions?

Regarding the issue of anonymisation of data, data security and complete anonymisation cannot be guaranteed even in non-profit research contexts. In practice and principle, data can be re-identified or stolen from the most secure clinical data warehouses. However, the cry for a total anonymisation of data in research settings might arguably proceed from a false premise. When data analysis turns out to have a positive impact on diagnostics and

[2] Technically, from a legal perspective, personal data is not subject to property rights and hence cannot be "owned".

therapies, the benefits outweigh the risks. Since other risks are accepted in society, the intense debates on data safety risks might even seem disproportionate. When there is clear evidence for a direct personal benefit, the normative stance on total anonymisation (or its modern core value of privacy) as a principle could even lose its validity and persuasiveness. A context-specific "micro ethics" might lend ethical legitimacy to health-related surveillance when evaluating its necessity, purpose and intent (Sewell & Barker 2007).

HYBRID AGENCY LEADS TO HYBRID RESPONSIBILITY

Hopes are high for the implementation of so-called AI in diagnostics or medical decision-making: it is likely that well-trained algorithms will one day outperform a human physician in applying the latest, most relevant medical research, in providing the most accurate diagnoses or in making the best decisions when choosing the most beneficial therapy. They might be deployed in order to reduce the number of errors made by humans in healthcare. Even though algorithms bear an inherent risk of making incorrect determinations, in many other areas and applications they make fewer mistakes than humans. The self-learning nature that is characteristic of machine learning systems, which are an authority in their own right in decision-making processes, effectively turns them into "autonomous moral agents" (Wallach & Allen 2009). This gives rise to an ethical question that is being fiercely debated at present: when the use of algorithm-based decision-making systems leads to incorrect conclusions that have detrimental consequences for the health of the individual patient or groups, who should be held responsible?

The most straightforward answer to this is probably that the company providing the algorithm should be held responsible for inaccurate results, ineffective therapies and the dire consequences they entail. Also, the certification body – in other words those who test and evaluate innovations – should share the responsibility for faulty technologies.

Yet the responsibility question becomes more complicated when the treating physician double-checks the results or decisions provided by the algorithmic system, which should always be the case. How much of the responsibility should she or he bear? Medical associations demand that the final decision must always lie with the doctor. The potential that is currently attributed to automated decision-making systems in the medical context leads to an unprecedented scenario: what if algorithms can prove that a physician's bad decision had harmful consequences for a patient?

So should the responsibility ultimately lie with the individual patient, who can decide whether to trust the doctor or the technology? If the beneficence of machine learning based decision-making and diagnostics can be statistically proven, what ethical principle should apply if patients choose to renounce these possibilities? Should doctors abandon diagnostic tools when a patient wishes them to do so?

A continuity argument might emphasise that the question of responsibility is not unprecedented, since previous innovations in the field of diagnostics or treatment (e.g. MRI, CT) also gave rise to concerns about unforeseeable risks and long-term side effects. Yet, with autonomous moral agents such as algorithmic decision-making systems, there is reason to believe that the innovative technology in question is categorically different from previous ones. This primarily concerns their considerably heightened degree of agency.

Technology – in both an instrumental and conceptual sense – is often used to delegate responsibility from human agents. However, social consequences are never caused by human or technological agents alone but emerge in their interaction. Agency, therefore, is hybrid, distributed between human and non-human agents.[3] The ethical relevance of this argument translates hybrid agency into the notion of hybrid (or shared) responsibility, since accountability, responsibility or morality can no longer be attributed to one defined entity (such as an "individual", a "subject" or "a machine"), but is distributed within dynamic networks of agency (Mittelstadt et al. 2016). The challenge of assigning agential responsibility in this network of "autonomous" technologies, technology producers and designers, and technology users becomes ever greater. Assuming a co-evolution of humans and technology in effect means that ethics and innovation co-evolve as well.

THE DILEMMA OF OVERDIAGNOSIS – IS IGNORANCE BLISS (AND WHO DECIDES THAT?)

The increasing use of machine learning tools in diagnostics, such as visual analytics in radiology, is very likely to produce more accurate results. At first glance, this seems to represent an overall improvement: the more accurate and the earlier a disease is diagnosed, the more effective the treatment and the more positive the patient outcomes. Also, these tools can easily be equally distributed, providing access to high-quality diagnostics with no expensive human expert necessary, even on a global scale. However, in applying these tools, a somewhat paradoxical line of conflict emerges between innovation and ethical principles.

Let us assume that a disease can be diagnosed with 100% accuracy and at a very early stage. With no symptoms being present, a hitherto perfectly healthy individual becomes – as a result of the diagnostic procedure (Mol 2002) – a patient, an individual who has no symptoms yet. Since a condition has been "discovered", however, there is an imperative to treat it. Depending on how invasive the treatment is, there is a greater

[3] Theoretical paradigms such as science and technology studies (e.g. Latour 1993) take this as an instrumental factor in the construction of social reality.

risk of it decreasing the patient's quality of life.[4] This problem may be aggravated by the use of so-called *predictive diagnostic* tools that make probability-based predictions about potential future medical conditions. Just knowing that they are likely to become ill has an impact on individuals' well-being. Should treatment therefore be started based on risk assumptions alone?

Hence, another responsibility concerns the principle of the long-term beneficence of AI tools rather than their accuracy and effectiveness. In other words, assessing their diagnostic validity is not enough, since it is crucial to address questions of clinical utility: do patients live longer, do they experience a higher quality of life? Otherwise, there is the risk of overdiagnosis, leading to overtreatment, with the sensitivity and accuracy of AI diagnostics causing more harm than good.

The responsibility for this decision cannot be left in the hands of either the individual physician and patient or with the provider of a diagnostics systems. These innovations pose the much more general question on what our collectively defined social and cultural limits for their use should be. In practice, it could be argued that the responsibility lies with those who test the long-term consequences of the diagnostic tools, who should conduct "fair" tests of whether an individual can expect to live a better life with or without the AI diagnostic tool.

The problem is to define the criteria that are put in place – what does "more good than harm" mean in practice? – and to determine who decides on them. This could even lead to a scenario in which diagnostic tests would have to be made deliberately less accurate or unavailable in situations where the quality of life would decrease for the majority of patients. What if one specific patient was part of a minority for whom quality of life increases? Who should decide on whether a test can be conducted or its results be discarded? For which groups would the test be defined as too precise? Who would determine when the variable "quality of life" attained a sufficient value to justify making the diagnostic reality known to physicians or patients? Should it be physicians who weigh the benefits against the diagnostic reality? Should it be patients who are given the opportunity to make these decisions for themselves?

Once these both highly ambiguous and consequential decisions are made, it might even be possible to automate and delegate them to the technology, for example, in the form of a test that only works when certain social and cultural variables are factored in and when an overall positive outcome is expected.

[4] The example of the well-known PSA test, which is used to identify a prostate-specific antigen (PSA) with the objective of detecting undiagnosed prostate cancer, is a case in point here. Despite the fact that it provides more accurate diagnoses, it is unclear whether using the PSA test reduces the mortality rate. This uncertainty is due to the side effects of surgery.

In the end, the ethical questions concern human agency and the criteria for socially, historically and culturally specific constructs such as "benefit", "harm" or "quality of life", which might differ greatly regarding the range of affected cultures, nations or social groups. Who has the authority to determine the social norms that are inscribed into the technology and the best practices for their deployment?

AUTONOMOUS PATIENTS, RESPONSIBLE INDIVIDUALS

The issue of knowledge is closely linked to individual autonomy, since it is always interwoven with power structures. Algorithmic agency – especially the agency emerging from self-learning systems – is not independent of social or cultural norms but is rather reflective of them in the results or decisions they produce. Biases are instilled into them, which includes the definitions of what is considered to be "healthy". Health is not just the absence of disease or the product of the ability to prevent or cure diseases. It is a contextual, value-laden, socially and culturally embedded construct.

Cultures of self-tracking and self-optimisation, together with discourses of risk management and mitigation in health and biomedical research, are to be understood as part of a larger neo-liberal market logic (Rose 2007). The universal datafication of our social lives makes it easy to implement more effective systems of patient surveillance and control. With the rising importance of data, patients are slowly transforming into "data subjects" who are kept under permanent surveillance (Lyon 2007); this creates new social and cultural categories, such as the various labels of being healthy, being "at risk" or being "not yet ill". This type of data categorisation always has social consequences as it is based on sorting and excluding certain groups or people. Even if you as an individual are not directly affected, your personal data might be part of a sorting mechanism or decision-making process.

Medical (self-)surveillance and tracking reinforce the idea that it is each individual's responsibility to stay healthy by improving his or her own lifestyle, nutrition and general fitness. Against the background of collective responsibility and solidarity, behaviour that is deemed irresponsible ceases to be an option (Rosengarten 2005), as can be observed in campaigns of obligatory vaccinations, health screenings or the debates on the donations of data or organs. Being a "responsible and healthy subject" may be in conflict with respecting an individual's desire and freedom to not know, perhaps even culminating in a form of resistance to the expectation to be productive, reproductive and healthy for the common good.

This type of self-governance can be a burden, promoting a machinistic image of the self, and it might profoundly transform our understanding of the concepts of health and illness altogether. When we are incessantly at risk of becoming ill, the actual state of well-being becomes secondary.

CONCLUSION

Evaluating technological innovation in terms of their risks and benefits in the field of digital health is not an easy task, since we need to take into account a multitude of different areas, each of which has unique ethical repercussions. Practices of data collection, analysis and surveillance come with both positive and negative implications for individuals and social groups; hybrid forms of agency and distributed responsibility make it increasingly difficult to ascribe accountability to individual stakeholders or the technology; knowledge can be empowering but also reflects and reinforces existing and often oppressive power structures, culminating in the requirements of self-surveillance and self-governance in seemingly liberal societies.

None of these ethical challenges can be solved by focusing on technologies alone, as these will undoubtedly evolve in accordance with existing social structures in the present system, which is dominated by a free-market logic constituted by stakeholders such as insurers, pharmaceutical and technological companies. Key to addressing the ethical issues is uncovering the underlying social problems that are merely reflected in – but never solved by –innovative technologies.

BIBLIOGRAPHY

Andrejevic, M. (2007). *iSpy: Surveillance and Power in the Interactive Era.* Lawrence: University Press of Kansas.

Ajana, B. (2017). Digital Health and the Biopolitics of the Quantified Self. *Digital Health, 3*(1), 1. doi:10.1177/2055207616689509

Fairfield, J. A. (2017). *Owned. Property, privacy, and the new digital serfdom.* Cambridge: Cambridge University Press.

Latour, B. (1993). *We have never been modern.* Harvard University Press.

Lyon, D. (2007). Everyday surveillance: personal data and social classifications. In S. Hier, P. Sean, & J. Greenberg (Eds.), *The Surveillance Studies Reader* (pp. 136-146). Maidenhead: Open University Press.

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society, 3*(2), 1–21.

Mittelstadt, Brent Daniel/Floridi, Luciano (2016): The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts. *Science and Engineering Ethics, 22*(2), 303–341. doi:10.1007/s11948-015-9652-2.

Mol, A. (2002). *The Body Multiple. Ontology in Medical Practice.* Durham/London: Duke University Press.

Prainsack, B. (2017). *Personalized Medicine. Empowered Patients in the 21st Century?*. New York: NYU Press.

Rose, N. (2007). *The Politics of Life Itself. Biomedicine, Power and Subjectivity in the Twenty-First Century.* Princeton/Oxford: Princeton University Press.

Rosengarten, M. (2005). The Matter of HIV as a Matter of Bioethics. In M. Shildrick, & R. Mykitiuk (Eds.), *Ethics of the Body. Postconventional Challenges* (pp. 71-90). Cambridge, Mass./London: MIT Press.

Sewell, G., & Barker, J. R. (2007). Neither good, nor bad, but dangerous: Surveillance as an ethical paradox. In S. P. Hier & J. Greenberg (eds.), The surveillance studies reader (pp. 354–367). Maidenhead: Open University Press.

Strohm Kitchener, K., & Anderson, S. K. (2011). *Foundations of ethical practice, research, and teaching in psychology and counselling.* New York, NY: Routledge/Taylor & Francis Group.

Wallach, W., & Allen, C. (2009). *Moral machines. Teaching robots right from wrong.* Oxford: Oxford University Press.

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

USES AND PERCEPTIONS OF EHEALTH APPLICATIONS

Seven cups to relieve stress? On the portrayal of well-being in the smartphone app market

FREYA SUKALLA AND VERONIKA KARNOWSKI

The portrayal of mental well-being apps in the app market may have serious negative implications, including exacerbating stigmatisation.

Keywords: well-being, mental health, smartphone apps, eHealth, qualitative content analysis

INTRODUCTION

Are you longing for a better and happier self? There is a plethora of smartphone applications available in app stores that promise to help you reach that goal. Many, if not most, of these apps would not intuitively be considered as health apps or even medical apps. Accordingly, they often are categorised using keywords such as lifestyle instead of health, fitness, or medicine. However, by targeting aspects of human or mental well-being, they do pertain to health as defined by the World Health Organization (1948).

Well-being can be understood as "optimal psychological functioning and experience" (Ryan & Deci 2001, 142). The concept is commonly differentiated into hedonic (or subjective) well-being and eudaimonic well-being. Hedonic well-being encompasses positive affect, an absence of negative affect, including stress and depression, and evaluations of life satisfaction (Diener 2000). In contrast, eudaimonic well-being captures psychological growth and the actualisation of one's potential, including self-acceptance, a sense of purpose in life, and positive social relationships (Ryff & Keyes 1995). Well-being is not only a part of health as defined by the World Health Organization (1948); research has also shown positive influences of well-being on overall health and longevity (e.g. Diener & Chan 2011; Ryff 2014). Hence, the promotion of well-being is a relevant means of increasing and supporting both overall health and especially mental health (WHO 2013).

As mental health is of growing concern worldwide, smartphone apps targeting mental well-being might make a meaningful contribution to preventative mental health (e.g., Howells, Ivtzan, & Eiroa-Orosa 2016). As these apps are highly accessible to users who are already using their phones to access health-related content (Fox & Duggan 2012), they may potentially empower users to take control of their own well-being (Albrecht 2016). At the same time, there are also risks of well-being apps. Just as the market for medical or clinical health apps has been characterised by a lack of evidence, privacy,

DOI: 10.5281/zenodo.3296991

and data security (Donker et al. 2013; Wang, Varma, & Prosperi 2018), the market for well-being apps, which is much less regulated (Terry & Gunter 2018), likely also suffers from the same problems, if not even more so. As such, it is plausible that some well-being apps might be harmful rather than beneficial, especially for vulnerable groups (Howells et al. 2016). Although well-being is beneficial in itself, the search for happiness may actually result in less happiness, with increased self-monitoring leading to increased self-focus and rumination (Gruber, Mauss, & Tamir 2011).

Hence some well-being apps could be detrimental to users who are already suffering from a mental illness or those who are in a vulnerable phase of psychological distress (Torous & Roberts 2017).

Moreover, it is important to go beyond looking at the effects of single apps and to consider the well-being app market as a whole. While this market has been little explored so far, the ecosystem of mental well-being apps likely contributes to notions of health, illness and well-being in society (Lucivero & Prainsack 2015; Lupton 2014). Just as the structure of the content we see when searching for information on the web shapes our attitudes and beliefs (as for example suggested by the concept of framing; Entmann 1993), we can assume that the type of information apps provide on a given topic will do just the same.

Applying these considerations, we investigate how mental well-being is conceptualised in smartphone apps targeting well-being. We focus on the definitions of well-being provided by these apps, the means suggested to achieve well-being and – given the potentially detrimental effects – the consideration given to both scientific evidence and warning notices on how to deal with mental health issues of clinical significance.

METHOD

To this end, we conducted a qualitative content analysis of the descriptive information provided about apps in app stores. Given that we did not assume any structural differences in apps provided by the two major app ecosystems, i.e. Google Play Store and Apple App Store, we concentrated on apps provided by the Google Play Store. In a first step, we used the German keyword for well-being – "Wohlbefinden" – to search for relevant apps. We then screened the first 100 apps in order to identify German apps exclusively focusing on some aspect of mental well-being with a view to conducting detailed analyses. After eliminating 33 non-German apps as well as 16 fitness apps exclusively focusing on physical exercise and 16 unrelated apps (e.g., office hour apps by fitness studios or doctors' offices), we coded the remaining 35 apps following a mixed inductive and deductive approach (Mayring 2014). Based on initial categories derived from our research question, we also allowed for new codes to emerge during coding.

RESULTS

Overall, our results show that the concept of well-being that is evident in the analysed apps can be easily mapped onto the academic conceptualisation of well-being (Ryan & Deci 2001). In line with the hedonic dimension, well-being is mainly described as a positive mental state, often in combination with physical health. At the same time, well-being also means achievement, positive social relationships, or, in some cases, self-optimisation, thus covering eudaimonic well-being. Regardless of whether an app targets hedonic, eudaimonic or both dimensions of well-being, there are generally two ways suggested to achieve mental well-being. The first includes meditation and mindfulness exercises, while the second involves self-monitoring (e.g. tracking physical activity, mood, sleep or goal achievement) with some form of feedback or even (algorithmic) coaching. However, the majority of app descriptions provide no information on scientific evidence for any of their efficacy claims. A few make vague references to "scientific studies" or "doctors and therapists". Only one of the 35 mental well-being apps analysed bases its claims on specific references to academic studies. Similarly, the issue of mental illness is rarely raised, and if it is, it is seldom addressed in sensible ways. Several apps even promise to alleviate depression, anxiety or addiction without a disclaimer of any kind. While our finding of a general lack of privacy and data security information mirrors prior results in the context of health apps (Albrecht 2016), it is also important to note the high costs for in-app-purchases and premium accounts for some of the apps in our sample as well.

CONCLUSION

To sum up our findings, we see that well-being apps on the Google Play Store target quite heterogeneous aspects of well-being, adequately reflecting the many dimensions of this construct. In contrast, the fact that mental well-being is portrayed as mainly achieved through meditation and self-tracking deserves critical attention. This implicitly promotes the idea that individuals are solely responsible for their well-being and mental health. By also failing to address any form of failure or the potential need for external (professional) help, these apps further contribute to a normative imperative of idealised self-help, which has serious implications for mental health and stigmatisation (Lupton 2014; Parker et al. 2018). First, the resulting social pressure not to feel sad or anxious and to take action could lead vulnerable individuals to experience more serious symptoms of mental illness and self-stigmatisation. On the other hand, this portrayal of mental well-being might also contribute to a stigmatisation of individuals with mental illnesses in society in general (Dejonckheere, Bastian, Fried, Murphy, & Kuppens 2017). This is especially relevant, as part of the stigma of many mental health disorders is the notion that sufferers are too lazy or weak (Mojtabai 2010).

Based on these limited initial findings, we therefore call for more scholarly attention to be paid to the well-being app market, its inherent structures and possible detrimental effects on users. Despite their exploratory nature, our findings clearly demonstrate the need to devote regulatory attention to the app market while at the same time educating users about the possibilities and limits of using well-being apps. Specifically, the establishment of a reliable certification system might prove valuable in the current German health app market, where such certification has not yet played any significant role (Albrecht, Hillebrand & von Jan 2018).

BIBLIOGRAPHY

Albrecht, U.-V. (2016). *Chancen und Risiken von Gesundheits-Apps (CHARISMHA) [Potentials and risks of health apps]* (report). Medizinische Hochschule Hannover. http://www.digibib.tu-bs.de/?docid=00060000

Albrecht, U.-V., Hillebrand, U., & van Jan, U. (2018). Relevance of trust marks and CE labels in German-language store descriptions of health apps: Analysis. *JMIR mHealth and uHealth, 6*(4), e10394. https://doi.org/10.2196/10394

Dejonckheere, E., Bastian, B., Fried, E. I., Murphy, S. C., & Kuppens, P. (2017). Perceiving social pressure not to feel negative predicts depressive symptoms in daily life. *Depression and Anxiety, 34*(9), 836–844. https://doi.org/10.1002/da.22653

Diener, E. (2000). Subjective well-being. The science of happiness and a proposal for a national index. *The American Psychologist, 55*(1), 34–43. https://doi.org/10.1037/0003-066X.55.1.34

Diener, E., & Chan, M. Y. (2011). Happy people live longer: Subjective well-being contributes to health and longevity. *Applied Psychology: Health and Well-Being, 3*(1), 1–43. https://doi.org/10.1111/j.1758-0854.2010.01045.x

Donker, T., Petrie, K., Proudfoot, J., Clarke, J., Birch, M.-R., & Christensen, H. (2013). Smartphones for smarter delivery of mental health programs: a systematic review. *Journal of Medical Internet Research, 15*(11), e247. https://doi.org/10.2196/jmir.2791

Entman, R. M. (1993). Framing: Toward clarification of a fractured paradigm. *Journal of Communication, 43*(4), 51-58. https://doi.org/10.1111/j.1460-2466.1993.tb01304.x

Fox, S. & Duggan, M. (2012). *Mobile health 2012*. PEW Research Center. http://www.pewinternet.org/2012/11/08/mobile-health-2012/

Gruber, J., Mauss, I. B., & Tamir, M. (2011). A dark side of happiness? How, when, and why happiness is not always good. *Perspectives on Psychological Science, 6*(3), 222–233. https://doi.org/10.1177/1745691611406927

Howells, A., Ivtzan, I., & Eiroa-Orosa, F. J. (2016). Putting the 'app' in happiness: A randomised controlled trial of a smartphone-based mindfulness intervention to enhance wellbeing. *Journal of Happiness Studies, 17*(1), 163–185. https://doi.org/10.1007/s10902-014-9589-1

Lucivero, F., & Prainsack, B. (2015). The lifestylisation of healthcare? 'Consumer genomics' and mobile health as technologies for healthy lifestyle. *Applied & Translational Genomics, 4,* 44–49. https://doi.org/10.1016/j.atg.2015.02.001

Lupton, D. (2014). Apps as artefacts: Towards a critical perspective on mobile health and medical apps. *Societies, 4*(4), 606–622. https://doi.org/10.3390/soc4040606

Mojtabai, R. (2010). Mental illness stigma and willingness to seek mental health care in the European Union. *Social Psychiatry and Psychiatric Epidemiology, 45*(7), 705–712. https://doi.org/10.1007/s00127-009-0109-2

Parker, L., Bero, L., Gillies, D., Raven, M., Mintzes, B., Jureidini, J., & Grundy, Q. (2018). Mental health messages in prominent mental health apps. *Annals of Family Medicine, 16*(4), 338–342. https://doi.org/10.1370/afm.2260

Ryan, R. M., & Deci, E. L. (2001). On happiness and human potentials: A review of research on hedonic and eudaimonic well-being. *Annual Review of Psychology, 52*(1), 141–166. https://doi.org/10.1146/annurev.psych.52.1.141

Ryff, C. D. (2014). Psychological well-being revisited: Advances in the science and practice of eudaimonia. *Psychotherapy and Psychosomatics, 83*(1), 10–28. https://doi.org/10.1159/000353263

Ryff, C. D., & Keyes, C. L. (1995). The structure of psychological well-being revisited. *Journal of Personality and Social Psychology, 69*(4), 719–727. http://doi.org/10.1037/0022-3514.69.4.719

Terry, N. P., & Gunter, T. D. (2018). Regulating mobile mental health apps. *Behavioral Sciences & the Law, 36*(2), 136–144. https://doi.org/10.1002/bsl.2339

Torous, J., & Roberts, L. W. (2017). The ethical use of mobile health technology in clinical psychiatry. *The Journal of Nervous and Mental Disease, 205*(1), 4–8. https://doi.org/10.1097/NMD.0000000000000596

Wang, K., Varma, D. S., & Prosperi, M. (2018). A systematic review of the effectiveness of mobile apps for monitoring and management of mental health symptoms or disorders. *Journal of Psychiatric Research, 107,* 73–78. https://doi.org/10.1016/j.jpsychires.2018.10.006

WHO (1948). Preamble to the constitution of the World Health Organization as adopted by the International Health Conference, New York, 19-22 June, 1946. https://www.who.int/about/mission/en/

WHO (2013). WHO mental health action plan 2013–2020. World Health Organization, Geneva. https://www.who.int/mental_health/publications/action_plan/en/

Technology acceptance, interest in fitness and empowerment: Testing consumer responses towards a wearable technology advert

ISABELL KOINIG AND SANDRA DIEHL

Keywords: TAM, advertising for new technologies, advertising effectiveness, wearables

INTRODUCTION

At a time when new technologies are constantly present, individuals' health has taken centre stage. A shift towards a performance society has affected individuals' professional and personal lives (Hillert & Marwitz 2006). In particular, the omnipresence of social media and new technologies is fostering both "self-surveillance" and "self-optimisation" and also a new form of "self-presentation", which is not without risks. The term "life logging" is commonly used to describe the continuous documentation of data that is used to discipline the human body to quantify the self (Selke 2013). According to Mau (2017), metric data has suddenly become a desired social value.

Conditioned by the introduction and continuous growth of wearable devices, consumers' interest in fitness and sport has risen. The data generated through the use of wearables is vital; it has the potential to involve individuals more strongly in their health care and ultimately to empower them (Hsiao and Chen 2018). At present, wearables are being used by almost one third of the US population (Statista 2018), and their use is predicted to increase in the near future: by 2022, the sales volume of wearables and fitness trackers is expected to amount to 190 million pieces (Statista 2018). This significant increase has been attributed to the ever-broadening scope of these gadgets' functionalities; they offer individuals a lot of health-related benefits and enable them to optimise individual performance as well as offering viable input to insurance companies, doctors and commercial companies (Wang et al. 2016). Yet it is unclear whether this number will be reached since data security and privacy are still listed as the prime reasons for why consumers refrain from using wearables altogether (Goodyear et al. 2017).

INVESTIGATING THE POTENTIAL OF WEARABLES

While wearables use is on the rise, the number of studies addressing these new gadgets and their relevance to individual health is still limited. Huberty and colleagues (2015) investigated how inactive middle-aged women reacted to wearable sensors and found

DOI: 10.5281/zenodo.3297019

that, while ease of wear and the instant availability of information were seen as positive, the use of wearables had some downsides, such as the device's appearance and weight. Contrary results were found by Melton et al. (2016), who determined that wearables did not improve students' physical activity levels and sleep patterns. Following Freedson et al. (2012), these results could be attributed to the users' uncertainty as to what constitutes a proper wear time as well as the exact features of the device. These findings are in line with a study by Kerner and Goodyear (2017), who found that wearables "wear out" quickly; for instance, in the case of adolescents, individuals stopped using these devices if they did not manage to perform well in peer comparisons, which were often perceived as acts of surveillance and regulatory actions (Goodyear et al. 2017). Negative consequences can also be explained by motivation-hygiene theory (Herzberg 1959), whereby hygiene factors, such as system unreliability or routine constraints, might have prompted users to discontinue their use of the gadget (Buchwald et al. 2018).

While wearables may be beneficial to the users' health, many people are still unaware of their potential and functions; therefore, it is important to advertise their benefits. To the authors' knowledge, no study so far has investigated how they can be promoted and whether consumers' attitudes towards fitness and their attitudes towards new technologies might play a role in ad evaluation and behavioural intentions.

Additional research has addressed which aspects consumers are particularly interested in when learning about wearables. According to Hsiao and Chen (2018), (hedonic and utilitarian) usability constructs deserve consideration and might help to positively shape consumers' attitudes towards new technological devices. Likewise, research on health and sport has confirmed that advertising messages are more effective when they include hedonic elements, which are able to literally "draw in" consumers (Hong et al. 2017), alongside utilitarian values (Hong et al. 2017). Consequently, advertisers are advised to highlight how their products benefit and empower consumers in their daily routines (Parreno et al. 2013). For instance, advertisements stressing "perceived value" were found to increase not only the image of the promoted gadget but also the product's performance value (Yeh et al. 2016). Yet messages were most successful when they also integrated utilitarian aspects, as suggested by motivation theory (Venkatesh et al. 2003), since both intrinsic and extrinsic motivation (usefulness vs. enjoyment) are presumed to impact consumers' attitudes towards new technologies.

While wearables may be beneficial to users' health, their potential and functions are still unknown to many people; therefore, it is important to advertise their benefits. Nonetheless, the practice of advertising is not without criticism, as commercial messages for all kinds of products have been found to be deceiving and misleading, a problem that has even led to legal action (Top Class Actions 2019). To the authors' knowledge, no study so far investigated whether and how consumers' attitudes towards fitness and the attitudes towards new technologies influence consumers' ad evaluation and behavioural

intentions regarding a promoted wearable product as well as the extent to which the information contained in an ad can empower consumers.

STUDY PURPOSE

Thus, the present contribution seeks to develop a conceptual model whose main components are derived from self-determination theory (Ryan & Deci 2000; Mears & Kilpatrick 2008), the technology acceptance model (TAM; Davis 1985), the classical (persuasive hierarchy) ad evaluation model (Petty & Cacioppo 1981) and the consumer-self-empowerment model (Koinig 2016; Koinig et al. 2017). While technology acceptance has already been linked to fitness trackers and wearable technology (Spagnolli et al. 2014; Sol & Baras 2016), to date, no study dealing with these gadgets has taken advertising as a starting point when it comes to studying consumer empowerment.

CONCEPTUAL MODEL

The proposed model intends to establish whether consumers' attitudes towards fitness impact their evaluations of a YouTube ad promoting a fitness tracker (H1a), their product evaluations (H1b) and their purchasing intentions (H1c). Consumers' attitudes towards new technologies are predicted to influence their ad evaluation (H2a), product evaluations (H2b), as well as their purchase intentions (H2c). Moreover, consumers' ad evaluations are not just predicted to influence their product evaluations (H3a), which are then expected to influence their purchasing decisions (H4); consumers' direct responses towards the ad are also assumed to empower them to better understand the product's functionalities or its use (H3b). If consumers feel empowered and enabled, this is also presumed to positively shape their product evaluations (H5a) and their intentions to purchase the fitness tracker (H5b).

STUDY POPULATION AND STIMULUS AD DESIGN

For the present study, a total of 156 subjects were recruited in a mid-sized European city in spring 2018. In terms of age, respondents were between 18 and 66 years old. Women constituted around 60% of the total sample.

An existing Fitbit ad promoting the Fitbit Ionic served as the study's stimulus material.[1] The advert was 21 seconds long and was chosen because it emphasised the device's capacity to support users and empower them in their day-to-day business.

[1] The actual advert can be found at https://youtu.be/F7qqtq9sLCo.

All hypotheses were tested simultaneously for the complete dataset using IBM SPSS AMOS Version 25. The proposed model shows acceptable global fit measures (CFI = .939; IFI = .941; CMIN/DF = 1.700; RMSEA = .048).

STUDY RESULTS

Study results revealed that consumers' attitudes toward fitness (M=5.6154) did indeed exert a positive impact on their ad evaluations (r=.284, p=.000) as well as on their purchasing decisions (r=.181, p=.000), supporting hypothesis H1a and H1c. However, this variable did not impact consumers' product evaluations (r=-.038, p =n.s.), and, thus, hypothesis H1b has to be rejected. Consumers' attitudes towards new technologies (M=4.7286) were found to influence their ad evaluations (r=.236, p=.004), but they were not found to have an impact on their product evaluations (r=.055, p=n.s.) or on their purchasing intentions (r=-.029, p=n.s.). So, hypothesis H2a is confirmed, whereas hypotheses H2b and H2c are rejected. Consumers' evaluations of the ad (M=4.7228) were found to both positively shape their product evaluations (r=.482, p=.000; M=5.0304) and to empower them (M=4.2821). This means that the ad enables consumers to better understand the product and its features (r=.696, p=.000). Consequently, both hypotheses H3a and H3b are supported. Our analyses also confirm the direct influence of product evaluation on purchase intention (r=.613 p= 000; M=4.2949), lending support to hypothesis H4. And while consumers' product evaluations are linked to the empowerment they receive from the ad (r=.293, p=.005), this empowered state does not lead them to purchase the product (r=.025, p=n.s.). Thus, while hypothesis H5a is affirmed, hypothesis H5b has to be rejected.

DISCUSSION OF RESULTS AND IMPLICATIONS

The study's results underline that consumers' attitudes towards fitness do indeed influence their ad evaluations and purchasing intentions. In spite of the lack of a direct connection between attitude towards fitness and product evaluations, we find an indirect influence (via ad evaluation), rendering recipients' attitudes towards fitness a viable variable in the conceptualised model. While consumers' attitudes towards new technologies influenced their ad evaluations, they did not impact their product evaluations or purchasing intentions. Empowerment was linked to ad evaluations, and, in turn, influenced consumers' product evaluations. Once again, we only found evidence of an indirect influence on purchasing intentions (via product evaluation). In addition, the direct connection between product evaluations and purchasing intentions could be confirmed. For advertisers

promoting wearables and fitness products, the implications are as follows: given that consumers often lack guidance as to what to expect from wearables – as indicated in previous studies (Melton et al. 2016; Freedson et al. 2012; Buchwald et al. 2018) – marketers are advised to empower consumers by highlighting their gadgets' functionalities and specifics (i.e. utilitarian values) and emotional side (i.e. hedonic aspects) in their advertising messages (Hong et al. 2017; Venkatesh et al. 2003); this will enable them to make educated and informed purchasing decisions based on message characteristics. Yet, advertisers benefit from transparency and would benefit from self-regulating industry standards that guarantee the truthfulness of advertising content and also disclose how consumers' personal data is used. This is crucial given wearables' increasing importance and broader spectrum of use (IDC 2017).

LIMITATIONS AND DIRECTIONS FOR FUTURE RESEARCH

There are several limitations to this study. First, the investigation was based on a rather small sample, limited to Germany and only looked at how consumers responded to one (online) advert. For this reason, we recommend not only replicating but also expanding the present study to different countries and for different ad stimuli; further research could also investigate whether certain response patterns are subject to cultural specifics. Future studies might also want to take socio-demographic parameters, including sex, age, or education, into consideration.

BIBLIOGRAPHY

Buchwald, A., Letner, A., Urbach, N., & von-Entreß-Fürsteneck, M. (2018). Insights into personal ICT use: understanding continuance and discontinuance of wearable self-tracking devices. Paper presented at the 26th European Conference on Information Systems, Portsmouth, UK. June 2018.

Davis, F. (1985), A technology acceptance model for empirically testing new end-user information systems - theory and results, PhD thesis, Massachusetts Inst. of Technology.

Freedson, P., Bowles, H.R., Troiano, R., & Haskell, W. (2012). Assessment of physical activity using wearable monitors: recommendations for monitor calibration and use in the field. Medicine and Science in Sports and Exercise. 44(1; Supplement 1), 1–4.

Herzberg, F. (1959). The motivation to work. 2nd ed. New York: Wiley.

Hillert, A. & Marwitz, M. (2006). Die Burnout-Epidemie oder brennt die Leistungsgesellschaft aus? München: C.H. Beck.

Hong, J.C., Lin, P.-H., & Hsieh, P.-C. (2017). The effect of consumer innovativeness on perceived value and continuance intention to use smartwatch. Computers in Human Behavior 67(February), 264-272.

Hsiao, K.L. & Chen, C.-C. (2018). What drives smartwatch purchase intention? Perspectives from hardware, software, design, and value. Telematics and Informatics 35, 103-113.

Huberty, J., Ehlers, D.K., Kurka, K., Ainsworth, B., & Buman, M. (2015). Feasibility of three wearable sensors for 24 hour monitoring in middle-aged women. BMC Women's Health. 15(55), DOI 10.1186/s12905-015-0212-3.

IDC. (2017). Worldwide Wearables Market to Nearly Double by 2021, According to IDC. Retrieved from: https://www.idc.com/getdoc.jsp?containerId=prUS42818517 [accessed 01.12.2018]

Kerner, C. & Goodyear, V.A. (2017). The Motivational Impact of Wearable Healthy Lifestyle Technologies: A Self-Determination Perspective on Fitbits with Adolescents. American Journal of Health Education 48(5), 287-297.

Koinig, I. (2016). Pharmaceutical Advertising as a Source of Consumer Self-Empowerment: Evidence from Four Countries. Wiesbaden: Springer.

Koinig, I., Diehl, S. & Mueller, B. (2017). Are pharmaceutical ads affording consumers a greater say in their health care? The evaluation and self-empowerment effects of different ad appeals in Brazil. International Journal of Advertising 36(6), 945-974.

Lupton, D. (2015). Data assemblages, sentient schools, and digitized health and physical education. Sport, Education, and Society 20, 122-132.

Mau, S. (2017). Das metrische Wir: Über die Quantifizierung des Sozialen. Berlin: Suhrkamp.

Mears, J. & Kilpatrick, M. (2008). Motivation for Exercise: Applying Theory to Make a Difference in Adoption and Adherence. ACSM's Health and Fitness Journal 12(1), 20-26.

Melton, B.F., Buhman, M.P., Vogel, R.L., Harris, B.S., & Bigham, L.E. (2016). Wearable Devices to Improve Physical Activity and Sleep: A Randomized Controlled Trial of College-Aged African American Women. Journal of Black Studies 47(6), doi. org/10.1177/0021934716653349.

Parreño, J. M., Sanz-Blas, S., Ruiz-Mafé, C., & Aldás-Manzano, J. (2013). Key factors of teenagers' mobile advertising acceptance. Industrial Management & Data Systems 113(5), 732–749.

Petty, R. A. & Cacioppo, J. T. (1981b). Attitudes and Persuasion: Classic and Contemporary Approaches. Dubuque, IA: William C. Brown.

Piwek, L., Ellis, D.A., Andrews, S., & Joinson, A. (2016). The rise of consumer health wearables: promises and barriers. PLoS Medicine. 13(2): e1001953.

PWC. (2016). The Wearable Life 2.0: Connected living in a wearable world. Retrieved from: https://www.pwc.com/ee/et/publications/pub/pwc-cis-wearables.pdf [accessed 01.12.2018]

Pyun, D. Y. & James, J. D. (2011). Attitude toward advertising through sport: A theoretical framework. Sport Management Review 14(1), 33–41.

Ryan, R. M. & Deci, E. L. (2000). Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. American Psychologist 55, 68-78.

Schwarz, E. C., Hunter, J. D., & LaFleur, A. (2013). Advanced theory and practice in sport marketing (2nd ed.). New York: Routledge.

Selke, S. (2013). Lifelogging als soziales Medium? – Selbstsorge, Selbstvermessung und Selbstthematisierung im Zeitalter der Digitalität. In: Jähnert, J. and Förster, C. (eds.). Technologien für digitale Innovationen. (173-200). Wiesbaden: Springer.

Shavitt, S., Lowrey, P., & Haefner, J. (1998). Public attitude toward advertising: More favorable than you might think. Journal of Advertising Research 37(4), 325–343.

Sol, R. & Baras, K. (2016). Assessment of Activity Trackers. Proceedings of the 2016 ACM Joint Conference on Persuasive and Ubiquitous Computing Adjunct. New York: ACM Press. 570-575.

Spagnolli, A., Guardigli, E., Orso, V., Varotto, A., & Gamberini, L. (2014). Measuring User Acceptance of Wearable Symbiotic Devices: Validation Study across Application Scenarios. In: Jacucci, G., Gamberini, L., Freeman, J., and Spagnolli, A. (eds.). Symbiotic Interaction. (87-98). Cham: Springer.

Statista. (2018). Prognose zum Absatz von Wearables weltweit von 2014 bis 2022 (in Millionen Stück). Retrieved from: https://de.statista.com/statistik/daten/studie/417580/umfrage/prognose-zum-absatz-von-wearables/ [accessed 01.12.2018]

Technopedia. (2019). Wearable Device. Retrieved from https://www.techopedia.com/definition/31206/wearable-device [accessed 12.03.2019]

Wang, J.B., Catmus-Bertram, L.A., Natarajan, L., White, M.M., Madanat, H., Nichols, J.F., Ayala, G.X., & Pierce, J.P. (2016). Wearable Sensor/Device (Fitbit One) and SMS Text-Messaging Prompts to Increase Physical Activity in Overweight and Obese Adults: A Randomized Controlled Trial. Telemedicine and eHealth, 21(10), 782-792.

Yeh, C.H., Wang, Y.-S., & Yieh, K. (2016). Predicting smartphone brand loyalty: Consumer value and consumer-brand identification perspectives. International Journal of Information Management 36(3), 245-257.

Yu, J., Lee, H., Ha, I., & Zo, H. (2017). User acceptance of media tablets: An empirical examination of perceived value. Telematics and Informatics 34(4), 206-223.

Family physicians' perceptions of the impact of e-visit systems on patient perceptions of and interactions with their family physicians

GALIT MADAR, AZI LEV-ON, NACHMAN ASH

INTRODUCTION

Information and communication technologies in general, and specifically eHealth systems, have penetrated the field of health on a significant scale in recent decades, transforming the relationships between physicians and their patients (Wehbe, Curcio, Gajjar, & Yadlapati 2015). The research on eHealth, however, has mainly focused on the uses and effects of *the internet and social media*. Conversely, the current study explores the effects of *eHealth system* use on the relationships between physicians and their patients and on patients' image of physicians' professional identities as viewed by physicians.

The internet and social media offer patients a broad range of opportunities to maintain their health, for example, by searching for information online or joining an online support group (Lupton 2013). Other health-related digital tools that have attracted less research attention include e-visit systems, which enable patients to communicate with their physicians, and allow physicians to access and manage patients' health-related data. These tools facilitate the provision of medical services without necessitating a visit to the physician's office (Wehbe et al. 2015).

The implications of these systems for the healthcare field are in dispute and have not yet been fully determined. For example, a study conducted in the United States (Padman, Shevchik, Paone, Dolezal, & Cervenak 2011) on adoption of e-visit systems by family physicians found that 50% believed that a face-to-face meeting is still the best way to diagnose their patients. However, according to the same study, 82% of the system's requests were dealt with within two correspondences, after which the patients received a proper medical diagnosis and treatment. The family physicians also mentioned that such systems have an essential role in modern medicine; they have the potential to make medical treatment more accessible, to improve patients' health and medical services and to reduce medical costs. A study by Leung & Chen (2017) reported that e-visit systems improved medical treatment efficiency, continuity and quality and physicians' availability.

MEDIATISATION AND PROFESSIONAL IDENTITY APPROACHES

The current study is grounded in a dual theoretical framework. First, *mediatisation theory* provides a paradigm for understanding changes in physician-patient relationships.

DOI: 10.5281/zenodo.3297079

According to the theory, the media constitutes a powerful social institution with its own logic (*media logic*), and other social institutions adapt to this logic (Hjarvard 2008; Mazzoleni 2008). Studies show that the media, and specifically social media, have become mediators in relationships in diverse fields, including relations with family and friends (Couldry and Hepp 2013). Still, to the best of our knowledge, ours is the first to apply it to the field of healt, and specifically to physician-patient relations.

Second, we also refer to a theoretical body of knowledge concerning *professional identity*. Professions are characterised by specialisation in a given body of knowledge and the use of unique language (Rodrigues et al. 2014). The medical profession is an organised therapeutic profession that applies and imparts knowledge in reference to health and sickness. In their training, physicians acquire information about the human body, health and sickness. They learn how to operate medical devices, analyse medical data and develop diagnoses. Physicians in training also internalise values, such as care for patients' well-being, respect for patient autonomy and the importance of social justice. Together, these structure physicians' professional identities (Freidson 1988).

Physicians' professional image may be challenged by social, technological and other changes, such as the contemporary re-conceptualisation of health organisations as service providers and their consequent focus on the quality of service rendered to patients (Robinson et al. 2009). This image may also be altered on professional, interpersonal and therapeutic grounds. This paper asks whether a physicians' image as the possessor of proper knowledge, as a personal authority who, starting at the time of the encounter, determines the clear boundaries and controls of the discourse and as a caregiver who meets in person with the patient have been altered as a result of the widespread introduction of e-visit systems.

Hence, the research questions for the current study are:

- What changes have occurred in the physician-patient relationship as a result of their computer-mediated communications?
- How does the use of online eHealth systems affect patients' perceptions of physicians' professional identity in physicians' view?

RESEARCH ENVIRONMENT

In 2012, Maccabi Health Services introduced an e-visit system that allows patients and physicians to communicate on a secured online network, creating online text-only medical "meetings". Six years after the system's introduction, 20% of all patient inquiries to physicians take place via the system. The online e-visit services are available for non-emergency medical care and work as follows: the patient accesses the organisation's online system and sends a written request to her physician. When the physician receives

the request, the patient's entire medical history is accessible and helps the physician to provide an appropriate response (Mehrotra, Paone, Martich, Albert, & Shevchik 2013).

STUDY POPULATION

The study was conducted in conjunction with Maccabi Healthcare Services. Maccabi provided a list of all affiliated physicians who regularly use its e-visit system. The researchers contacted 100 physicians by SMS. Interviewees were selected to represent a diverse sample of family physicians affiliated with Maccabi in terms of scope of use, geographic location and gender. The interviews were conducted face-to-face at the doctors clinic.

The study population included 25 family physicians (11 male, 14 female) between the ages of 37 and 70 (M = 49.52, SD = 10). Physicians' tenure ranged from 5 to 32 years (M = 20.33, ST = 11.33). The majority (60%) of the physicians were native Hebrew speakers.

METHODOLOGY

The study was based on semi-structured in-depth interviews, designed to tap into interviewees' descriptions of the phenomenon under investigation from the physicians' perspective in their own words. The interviews focused on the following aspects: the benefits and drawbacks of e-visit systems, the possible over-use of the system, the position of the family physician, the possible transformation of patient-physician interactions as a result of the e-visit system, physician attitudes toward the system and the way the family physician perceive his role following the use of the e-visit system.

A thematic analysis (Broom & Dozier 1990) was used to analyse the data collected in this study. This analysis was based on an inductive, open-ended coding process designed to identify the topics that emerge from the interviewees' statements.

FINDINGS

Theme 1: The physician as a professional: Patients' changing views of their physicians' professional image

The vast majority of physicians interviewed for this study stated that their use of the e-visit system had meant that *bureaucratic, administrative, and service-related tasks assumed a larger proportion of their work*. Physicians stated that their interactions with their patients had changed as a result: patients come to their interactions with more

knowledge and consequently more opinions and doubts about various treatment options and medications. As a result, physicians feel that they are frequently expected to act as clerks and that their professional insights are not required.

The interviewees indicated that most physicians feel as if they are service providers whose role it is to satisfy their patients' wishes: "The physician is no longer a professional who provides care; he is a service figure. Service has become more important than a physician's professional value" (#13). Occasionally patients communicate a list of demands to their physician and refuse to listen to her advice, as one interviewee noted, "When I get the feeling that he is [not listening to me] and starts to practice medicine, and starts to manage the medical treatment by himself, then I write to him: 'Please schedule an appointment in my office'" (#25).

Theme 2: The physician as an interpersonal authority

Many physicians stated that the system's convenience had encouraged a profusion of inquiries and fed patients' expectations of a rapid response, with little involvement required of the patients themselves. On this point, the majority of physicians reported the challenges of setting boundaries with their patients and their concerns with losing their authority status. This entailed challenges to their ability to control the appointments that take place in their offices and to manage the interactions with their patients.

For example, one of the interviewees stated: "My patients write: 'sick day approval for such and such date.' I ask them what the approval is for, what the problem is, and so it causes a bit of hassle for both of us…and sometimes I even feel uncomfortable if I ask them to come in and see me" (#5).

Theme 3: The physician as a medical practitioner

The physician-patient relationship has traditionally been based on interpersonal communications, confidentiality and relevant information conveyed by the physician to the patient (Mechanic 1998). Communicating properly and viewing the patient as a human being with an individual identity, aspirations, goals and desires helps build trust between the physician and the patient (Fiscella, Meldrum, & Franks 2004).

Many physicians stressed that online encounters cannot replace in-person appointments in the physician's office or clinic. When medical treatment takes place through an online system, the physician-patient relationship is compromised, and consequently, the doctor's perceived professional identity as a medical practitioner is negatively impacted. The physicians interviewed for this study argued that during face-to-face visits they also render quasi-psychological treatment, discuss preventive medicine issues relevant to the patient and promote the required health quality measures. This aspect of treatment is more difficult to render when physicians and patients communicate digitally.

According to the interviewees, "There is no substitute for observation, a glance, sometimes the patient needs an examination. You can't do everything by remote control.

Remote control is good, but it's not a substitute for a visit when a visit is necessary" (#16). "Sure, we want to see what you look like….You forget that we need to meet, sit down together and discuss your condition" (#1).

DISCUSSION AND CONCLUSIONS

The current study examined how an online e-visit system transformed patients' perceptions of and relationships with their physicians, as perceived by physicians. Three main themes emerged from the analysis of findings, which represent the key aspects of patients' perceptions of and relationships with their physicians that have been transformed by the extensive use of an e-visit system.

The physician's professional image: The physician is a professional authority who draws on her professional knowledge and skills. Interviewees argued that the use of the e-visit system accelerated a shift in patients' perception from a view of their physicians as professionals to a view of their physicians as service providers.

The physician's interpersonal authority: Physicians control the appointments that take place in their offices, and manage the interactions with their patients. In the online sphere, the physician does not see the patient, a fact that challenges her interpersonal authority. Physicians reported that, when managing the inter-personal communication in the e-visit system, they spend more time engaged in interaction management and boundary setting, while in the background a non-verbal message is being communicated to the physician that the patient does not wish to come to the physician's office in person.

The physician as a therapeutic practitioner: Findings of the current study highlighted the significance that the physicians attributed to the physical meeting between patients and physicians. Physicians stressed the importance of all aspects of the face-to-face encounter, including dialogue, observation, physical examination, touch and exploring the patient's condition and feelings, all of which are integral elements of treatment.

Future studies might compare the effects of e-visit system use with the effects of other eHealth systems in use worldwide. A future study might also examine physicians' perceptions of the implications of eHealth system use over time and provide a broader perspective on the benefits and challenges of extensively using such systems.

BIBLIOGRAPHY

Broom, G. M., & Dozier, D. M. (1990). *Using research in public relations: Applications to program management.* New Jersey: Prentice Hall.

Couldry, N., & Hepp, A. (2013). Conceptualizing mediatization: Contexts, traditions, arguments. *Communication Theory, 23*(3), 191-202.

Fiscella, K., Meldrum, S., Franks, P., Shields, C. G., Duberstein, P., McDaniel, S. H., & Epstein, R. M. (2004). Patient trust: is it related to patient-centered behavior of primary care physicians? Medical care, 42(11), 1049-1055.

Freidson, E. (1988). *Profession of medicine: A study of the sociology of applied knowledge.* Chicago: University of Chicago Press.

Hjarvard, S. (2008). The mediatization of society. *Nordicom Review, 29*(2), 102-131.

Leung, L., & Chen, C.C. (2017, June). *E-Health/m-Health Adoption and Lifestyle Improvements: Exploring the Role of Technology Readiness, the Expectation-Confirmation Model, and Health-Related Information Activities.* Paper presented at the 14th International Telecommunications Society (ITS). Asia-Pacific Regional Conference.

Lupton, D. (2013). The digitally engaged patient: self-monitoring and self-care in the digital health. *Social Theory & Health, 11*(3), 256-270.

Mazzoleni, G. (2008). Mediatization of society. *The international encyclopedia of communication.*

Mechanic, D. (1998). The functions and limitations of trust in the provision of medical care. *Journal of Health Politics, Policy and Law, 23*(4), 661-686.

Mehrotra, A., Paone, S., Martich, G. D., Albert, S. M., & Shevchik, G. J. (2013). Characteristics of patients who seek care via eVisits instead of office visits. *Telemedicine and e-Health, 19*(7), 515-519.

Padman, R., Shevchik, G., Paone, S., Dolezal, C., & Cervenak, J. (2010). eVisit: a pilot study of a new kind of healthcare delivery. *Studies in health technology and informatics,* 160, 262-266.

Robinson, J. C., Casalino, L. P., Gillies, R. R., Rittenhouse, D. R., Shortell, S.S., & Fernandes-Taylor, S. (2009). Financial incentives, quality improvement programs, and the adoption of clinical information technology. *Medical Care, 47*(4), 411-417.

Rodríguez, C., Pawlikowska, T., Schweyer, F. X., López-Roig, S., Bélanger, E., Burns, J., & Fiquet, L. (2014). Family physicians' professional identity formation: a study protocol to explore impression management processes in institutional academic contexts. *BMC medical education, 14*(1), 184-195.

Wehbe, R., Curcio, E., Gajjar, M., & Yadlapati, A. (2015). Technology and its influence on the doctor patient relationship. *International Cardiovascular Forum Journal,* 3, 38-39.

The corpus of author's interview data is available upon request.

"Self-management for better health? Reflections on the self-tracking culture"

NIKLAS TRINKHAUS

REPORT ON THE KEYNOTE BY BTIHAJ AJANA

Introduction to the problematic aspects of the growing self-tracking culture (not only) in the health sector.

Keywords: self-tracking, quantified self, neoliberal ethos, self-improvement, public good

The growing self-tracking culture is expected to be part of the solution to severe problems in the public health sector because it promises a personalised, participatory and preventive approach towards health. Even though there may be some benefits and positive outcomes of self-tracking, Btihaj Ajana's keynote aimed to "caution against the excessive optimism towards the role and the potential of self-tracking technologies".

SELF-TRACKING AND THE QUANTIFIED SELF

Self-tracking refers to the active gathering of everyday and health-specific data using smart technologies such as wearables and smartphones. The range of activities that can be tracked is immense and nearly endless: from sleeping patterns and exercise to sexual performance and eating habits. Almost everything can be measured and tracked. While any owner of a smartphone might consciously or unconsciously be tracking data in one way or the other[1], there is still a considerable difference from the self-tracking practices undertaken by the "quantified self" community, as Ajana pointed out.

The "quantified self" community is based on self-tracking but goes beyond this sole focus by being a proactive, organised and ideologically embedded culture that could also be described as a movement. Founded in 2007 by Kevin Kelly and Gary Wolf in the US, there are more than 200 groups in at least 34 countries that refer to themselves as quantified-self groups. They are characterised by a desire to improve various aspects of everyday life through quantification and numbers.

[1] For example, through the Apple Health App, which is pre-installed on iPhones and cannot be deleted.

DOI: 10.5281/zenodo.3297109

BECOME BETTER THAN YOU ARE

What could be problematic about the idea of improving your own health or well-being through data accumulation? According Btihaj Ajana, it is crucial to differentiate between those who already enjoy good health and aim to improve their fitness and those who suffer from certain diseases and use tracking devices to manage their condition and improve their health status. While the latter group seeks to cure or treat certain diseases (e.g. diabetes) the former is mostly driven by the promise "to become a better version of yourself". For Ajana, the optimisation of the self is one of the central motives of the quantified-self movement. While at first glance, this could be regarded as a motivating and empowering outcome of self-tracking, there are several downsides directly connected to such self-improvement imperatives.

On the one hand, such developments represent a general shift of responsibility for health in society (Swan 2012). It appears that the healthcare system and its professionals are no longer the key actors responsible for health and wellbeing. It is instead the individual who has to become responsible, proactive and enterprising towards health and life in general. For Ajana, this attitude runs in "parallel with the decline of state support for social and healthcare programs in general" and is reflective of a pervasive neoliberal ethos.

EMPOWERMENT OR ABANDONMENT?

The seductive promise of empowerment and control over one's health might, in the long run, turn out to be no more than the abandonment of the patient, as the burden of responsibility and decision-making is left to the individual, according to Ajana. Additionally, the required technologies cannot be used without meeting further conditions. In fact, it is necessary to possess a certain "digital capital" as Ajana noted with reference to Hampshire et al.'s (2015) arguments. "Digital capital" refers to the need for appropriate resources, skills and social networks to take advantage of the potential of a digitally mediated healthcare.

And is it even desirable to know every detail about one's own body and health? Critics like Ajana argue that excessive knowledge could result in over-diagnosis and -treatment. If every little health issue is detected, this may result in an exponential increase in (unnecessary) treatment and an explosion of health costs. This runs entirely contrary to the promise of a more cost-effective health system through self-tracking (see Welch 2012). Moreover, it may result in increasing anxiety and stress for individuals rather than autonomy and control. Sociologist Deborah Lupton describes this phenomenon as "Cyberchondria", a digitally enhanced version of hypochondria (Lupton 2013).

PUBLIC GOOD OR PRIVATE PROPERTY?

The discussion between those who advocate for the accumulation of health data and those who are sceptical about its benefits and outcomes is intense. Those who are in favour of the tracking culture regard their actions as a philanthropic contribution towards a humanistic goal: the promotion of a new type of medicine, individualised treatment and the cure of rare diseases. This is why the term data *philanthropy* was invented. The sharing of personal data is characterised as good citizenship that can contribute to a sense of public good. Furthermore, critics of data sharing are accused of being selfish and the whole concept of data protection as being egoistic (see also Ajana 2017).

Behind these terms of solidarity and betterment, Btihaj Ajana identifies something quite different. As the data are usually gathered by private companies, the concept of data philanthropy for public good turns out to be less romantic. The data are not accessible to the public and, what is more, not even to those who produce the data, as Ajana highlighted using the example of Fitbit and Strava. Fitbit, for example, used to charge 50 US dollars if consumers wanted to access their own data. So, what is promised to be a public good turns out to be a private property from which companies, rather than the public, benefit.

TRACK IT LIKE IT'S HOT (DATA)

Admittedly, the tracking of health data may have a positive impact on the treatment of certain diseases and especially for research purposes. For example, in the field of cancer research, hopes for better and faster curing rates through individual treatment is high. On the other hand, the tracking of sensitive health data may also result in undesirable outcomes: it may prompt a shift in responsibility towards the individual, the abandonment of patients, over-diagnosis and the privatisation of health data.

Thus, a public discussion is needed on the kind of data that should be gathered and what concept of health we are aiming for. If we're talking in terms of *public good*, it needs to be clarified who can access the data and for which purposes that data will be used. Then digitally mediated health may play an important role in the improvement of public health services.

BIBLIOGRAPHY

Ajana, B. (2017). 'Digital Health and the Biopolitics of the Quantified Self', Digital Health, vol. 3, no.1, 1-18.

Hampshire, K., Porter, G., Owusu, S. A., Mariwah, S., Abane, A., Robson, E., ... & Milner, J. (2015). Informal m-health: How are young people using mobile phones to bridge healthcare gaps in Sub-Saharan Africa?. Social Science & Medicine, 142, 90-99.

Lupton, D. (2013). 'Living the quantified self: the realities of self-tracking for health', https://simplysociology.wordpress.com/2013/01/11/living-the-quantified-self-the-realities-of-self-tracking-for-health/.

Swan, Melanie. (2012). Health 2050: The Realization of Personalized Medicine through Crowdsourcing, the Quantified Self, and the Participatory Biocitizen. Journal of personalized medicine. 2. 93-118. 10.3390/jpm2030093.

Welch. G. (2012). in 'The Measured Man', Boweden. M. The Atlantic: https://www.theatlantic.com/magazine/archive/2012/07/the-measured-man/309018/.

TECHNOLOGY AND INNOVATION IN CONTEXT

Second-order interoperability in the datafication of public health

MARTIN STOJANOV

This paper investigates the practical work of repurposing web search data for public health surveillance and highlights challenges related to interoperability.

Keywords: datafication, interoperability, public health, second-order friction

INTRODUCTION

With internet use becoming an integral part of many people's everyday lives, using the internet to obtain health information and engage in self-care is by now an established practice (Nettleton, Burrows & O'Malley 2005). Searching for health information online produces a data trace that consists of search terms and information on their distribution over time, which can be stored in the user's web browser as well as in the search engine's databases. Health-information seeking online and other online activities produce data traces of our actions, in a process that can be referred to as datafication (van Dijck 2014). This continually produces updating data sets, which can then be repurposed in different contexts (Newell & Marabelli 2015). Within the realm of public health, datafication is being adopted in syndromic surveillance – the practice of monitoring population health in order to formulate appropriate public health responses. Infodemiology exemplifies how web search traces, which often consist of search terms related to symptoms, are being used to identify a potential outbreak that could require a public health intervention (Eysenbach 2006).

Datafication, and with it the repurposing of data, is an example of a second-order system, meaning a system that relies on a network of (first-order) systems built for purposes other than those of the second-order system (Boyce 2016; Van Der Vleuten 2003). Second-order systems borrow from and are dependent on existing infrastructure, but they still maintain their own databases (Boyce 2016). Boyce (2016) has examined the public health infrastructure for surveilling foodborne disease outbreaks in terms of second-order systems, as it relies on data and materials repurposed from the food and health sector. She articulates some of the challenges they face through the notion of second-order friction, which brings to the fore the efforts involved in overcoming obstacles "when actors in the second-order system repurpose materials and data from other systems and infrastructures (Boyce 2016, 56)." One such challenge when repurposing diagnostic tests performed by different laboratories pertains to variations in testing approaches between the laboratories as well as variations over time, which can threaten interoperability (Boyce 2016).

DOI: 10.5281/zenodo.3297139

Interoperability is understood broadly as making "heterogeneous data work with each other (Ribes 2017 1515) " and entails the work of making data comparable according to a common metric or commensurable; it is an important factor for enabling reuse of data for disease surveillance in public health (Dixon, Vreeman, & Grannis 2014). Differences in what measures are used to diagnose patients could have an impact on whether repurposed diagnostic test data are comparable.

Interoperability in the context of the datafication of public health remains underexplored. The present paper adds to this discussion through a case study of the repurposing of data traces from health information seeking online for infodemiology. It examines the dependency of a second-order system in the context of the datafication of public health and looks at the implications for interoperability. It highlights second-order frictions with respect to the maintenance and development of the systems that the second-order system relies on in order to shed light on interoperability challenges for datafication in public health.

RESEARCH APPROACH AND RESEARCH SETTING

This paper comes from a larger study examining datafication in public health by following the development and use of an infodemiological system (hereinafter InfoSurv), which relies on data traces produced when individuals seek health information online. An automated analysis in InfoSurv of the proportion of searches that are related to a set of symptoms associated with seasonal illnesses allows epidemiologists to follow the incidence of illness in the population. When the relative number of search terms for symptoms related to influenza rise, epidemiologists consider it to be a signal that the incidence of influenza in the population has increased. InfoSurv is maintained by a Nordic public health organisation. It uses search data from a prominent health information portal (hereinafter HIP) to estimate illness in populations. The HIP website has a search bar for locating content, but many HIP visitors arrive at their desired webpage via a prominent search engine (hereinafter SE).

The study's methodology consisted of a participant observation of three developers who worked with maintaining and developing InfoSurv and of weekly meetings between five public health professionals whom InfoSurv factors into decision making about current influenza incidence. Informal interviews and document studies also supplemented the participant observation. While the larger study was initiated in September 2017, this paper focuses on a series of events surrounding changes to the HIP and how it affects InfoSurv; these unfolded between January and April 2019. As InfoSurv relies on stable search behaviour via the HIP search bar to find patterns indicating changes in the incidence of illness, a change in the HIP website risks creating a discontinuity with historical data and compromising its use. As of April 2019, the full implications of the changes to HIP were still unfolding.

EXPLORING ALTERNATIVE DATA SOURCES TO THE FIRST-ORDER SYSTEM

The extent of the planned changes to the HIP came to the attention of the developers in January 2019 and raised concerns that InfoSurv would no longer be able to operate. The HIP was to receive a new search engine, with a different way of providing search suggestions to users; this development could alter search patterns among future HIP visitors. Furthermore, the HIP website was to undergo design changes that could further alter the search patterns. Hence, the developers explored ways of mitigating the impact of the first-order changes on the second-order system.

The developers explored the possibility of using search data as an alternative data source for InfoSurv, which was originally developed using sentinel data on influenza-like illnesses and HIP data from the corresponding time period. The developers investigated whether the two datasets could be combined:

> **D1:** One of the problems is that we don't have enough historical data.
> **D2:** But perhaps we could adjust the historical data. But it's troubling that there is such a big difference in the search pattern for pregnancy.
> **D3:** Also fever and influenza.
> **D1:** So you're thinking that we could transform it?
> **D2:** It would have been easier if it wasn't so inconsistent. It's difficult to be confident with this difference.
>
> *(Adapted from fieldnotes)*

The difference between the HIP data and the SE data was too substantial and the inconsistencies too great for them to be reliably combined. Hence, the developers were not confident that the data sources were similar enough for the SE data to provide a solution.

A further limitation of the SE dataset pertained to the timing of its availability (see Figure 1 and Figure 2). Data for the full preceding week only became retrievable when there was a three-day delay instead of one, as had been the case with HIP data. If implemented with SE data, this delay would have affected existing influenza surveillance routines, which produced an analysis on Mondays based on the previous week and made an extrapolation for the current week on Wednesdays based on data from Monday and Tuesday of the same week. These analyses were discussed on Wednesdays in conjunction with other surveillance systems to assess influenza incidence. Furthermore, SE data was logged in Pacific Standard Time, which shifted the week in time due to the time differences. Basing InfoSurv on SE data would mean InfoSurv would no longer align with the definition of a week used in other surveillance systems.

The second-order system was developed from the data production of the first-order system. While the data from the SE could be acquired and the search terms mostly coincided with the HIP data, they could not be made to work together. To be a viable solution, the SE dataset needed to be made commensurable with the dataset from the HIP search bar. However, the model underpinning the surveillance system had been developed around a data stream constituted in the interaction between users and a particular HIP design. It also relied on the means of navigating that website with a particular search bar, such that one data source could not easily be aligned with another seemingly similar data source. This echoes the claims by Ribes (2017, 1516) that data interoperability is an arduously and historically inscribed accomplishment "still carrying the consequences of that interoperation to future uses."

Figure 1. Work practices based on HIP data

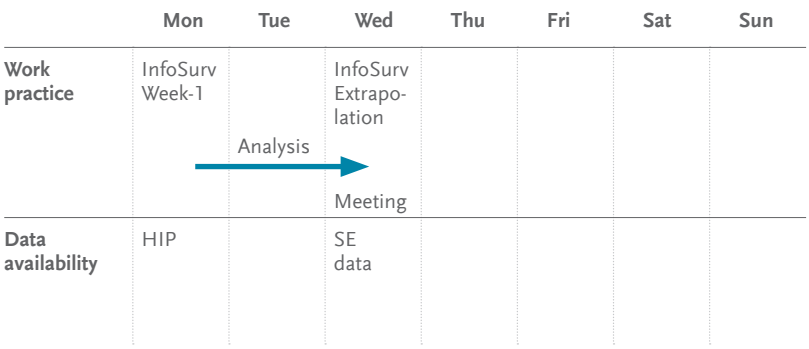
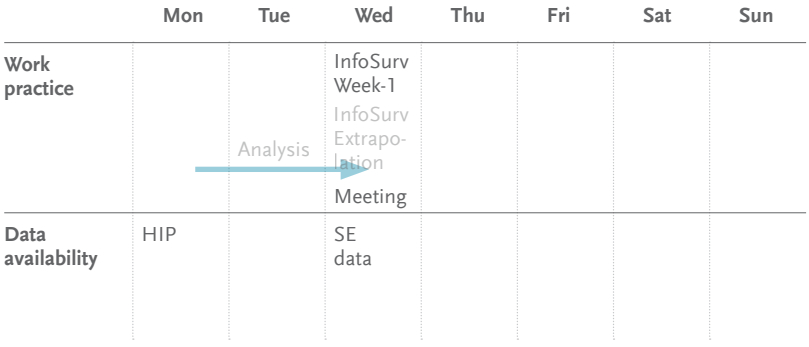


Figure 2. Work practices based on SE data



The findings also highlight the significance of spatio-temporality for the interoperability of data with respect to work routines and other surveillance systems. As work practices structure time (Orlikowski & Yates 2002), and in this case are co-constituted together with a range of other surveillance systems with an existing definition of "a week", it becomes difficult to integrate a new data source if it does not align with the existing temporal structures. Both of these vignettes speak to the sensitivity of datafication to consistency in the way data is generated. In this regard, InfoSurv is similar to lab-based surveillance systems. Boyce (2016) shows how changes in lab equipment can threaten interoperability in disease outbreak surveillance. The examples suggest that a new data source can be challenging with respect to interoperability and that there could be a tension between the continuation of InfoSurv and innovation in the systems from which data is repurposed.

MAINTAINING A CONNECTION IN THE FACE OF FIRST-ORDER CHANGE

In addition to exploring alternative solutions, the developers worked to adapt the second-order system to ensure that InfoSurv would be able to continue receiving HIP data after the HIP changes. Partly, this process meant revising the way in which the second-order system managed first-order maintenance routines. The search data that InfoSurv receives from HIP needs to be filtered to remove test searches done as part of HIP maintenance. Depending on when the HIP data was generated, InfoSurv parses it differently to account for the HIP maintenance routines that were in place at the time when the data was generated. The consultants working with the changes to HIP were forthcoming on how to identify maintenance routines in the upcoming version of HIP, but this had not always been the case. For certain parts of the historical data, the developer had to infer which search terms stemmed from maintenance testing based on patterns in the data, as the organisation responsible for maintaining the HIP at the time was unable to provide reliable information about who could be doing testing and when.

The new version HIP has also changed the way in which the HIP produces and delivers data about search behaviour: the new search engine distributes the computing workload between several servers, dynamically adapting depending on workload and creating one search log file for each active server instead of one search log file. This has created uncertainty about how to distinguish an unusually small number of log files, a problem that arises due to an error related to unusually low HIP use. During a meeting with the consultants, the developer raised the question of how to reliably determine that InfoSurv had acquired all the data for the previous day:

> **D1:** I'd like us to define how we ascertain the number of files so that we know if there is something missing. It's hard to look for something that does not exist.
> **Consultant:** Our focus is on delivering what we need to. We have quite a lot to do. We can deliver the files and if it turns out to be a problem we'll have to re-evaluate. I need to give you an answer that is a bit dissatisfying.
>
> *(Adapted from fieldnotes)*

At the time, the first-order system and second-order system were connected without a guarantee that all relevant data had been transferred. While there were agreements regulating the transfer of data from the first-order system to the second-order system, the means of enforcement were such that it was done on a voluntary basis.

The findings suggest that the first-order maintenance practices can influence the interoperability of data in the second-order system. Since the system maintenance routines of the first-order system can influence the production of the search data that are repurposed in the second-order system, changes in these routines can impact what data patterns emerge. Hence, datafication is continuously being repaired in order to maintain interoperation according to what first-order system maintenance routines are in place. The focus on repair work articulates how data interoperation in datafication is a continuous accomplishment (Jarzabkowski & Pinch 2013), one that is repeatedly and constitutively linked to second-order maintenance practices that (re-)align algorithms and data to compensate for first-order changes.

Much like Boyce (2016), the study finds that the impact of first-order changes on interoperability can vary. While the maintenance routines could be compensated for, the developers had more difficulty in managing the dynamic load balancing between different servers. This did not remain unresolved due to an inherent technical difficulty but rather due to differing priorities in the face of time pressure. Interoperability in the second-order system was prioritised only in so far as it did not interfere with first-order priorities. This suggests that, due to the asymmetric dependence of second-order systems (Boyce 2016), a careful examination is needed of how responsibilities and accountabilities for data transfer are arranged in order to ensure interoperability in the datafication of public health and a sensitivity to what agreements are put in place. Furthermore, both the example of the maintenance routines and the dynamic server loading highlight the significance of working relations in making data interoperate across the first- and second-order systems.

CONCLUSION

This paper has sought to unpack some of the second-order frictions in making datafication in public health work based on repurposed web search data. In particular, it highlights challenges of making data commensurable. The case suggests that interoperability in datafication is a continuous accomplishment that entails compensating for first-order modifications to the system that produces the repurposed web search data. Furthermore, changes in the system generating the data that is being repurposed can threaten data interoperation in ways that can be difficult to mitigate. It highlights that first-order maintenance routines, the spatio-temporality of data and its compatibility with work practices as well as the alignment between first-order and second-order priorities can have an impact on interoperability.

BIBLIOGRAPHY

Boyce, A. M. (2016). Outbreaks and the management of 'second-order friction': Repurposing materials and data from the health care and food systems for public health surveillance. *Science & Technology Studies*. Retrieved from https://sciencetechnologystudies.journal.fi/article/view/55409

Dixon, B. E., Vreeman, D. J., & Grannis, S. J. (2014). The long road to semantic interoperability in support of public health: Experiences from two states. *Journal of Biomedical Informatics, 49,* 3–8. https://doi.org/10.1016/j.jbi.2014.03.011

Eysenbach, G. (2006). Infodemiology: Tracking Flu-Related Searches on the Web for Syndromic Surveillance. *AMIA Annual Symposium Proceedings, 2006,* 244–248.

Jarzabkowski, P., & Pinch, T. (2013). Sociomateriality is 'the New Black': accomplishing repurposing, reinscripting and repairing in context. *M@n@gement, 16*(5), 579–592. https://doi.org/10.3917/mana.165.0579

Nettleton, S., Burrows, R., & O'Malley, L. (2005). The mundane realities of the everyday lay use of the internet for health, and their consequences for media convergence. *Sociology of Health & Illness, 27*(7), 972–992. https://doi.org/10.1111/j.1467-9566.2005.00466.x

Newell, S., & Marabelli, M. (2015). Strategic opportunities (and challenges) of algorithmic decision-making: A call for action on the long-term societal effects of 'datification.' *The Journal of Strategic Information Systems, 24*(1), 3–14. https://doi.org/10.1016/j.jsis.2015.02.001

Orlikowski, W. J., & Yates, J. (2002). It's about Time: Temporal Structuring in Organizations. *Organization Science, 13*(6), 684–700.

Ribes, D. (2017). Notes on the Concept of Data Interoperability: Cases from an Ecology of AIDS Research Infrastructures. *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing - CSCW '17,* 1514–1526. https://doi.org/10.1145/2998181.2998344

Van Der Vleuten, E. (2003). In Search of the Networked Nation: Transforming Technology, Society and Nature in the Netherlands during the Twentieth Century 1. *European Review of History: Revue Européenne d'histoire, 10*(1), 59–78. https://doi.org/10.1080/13507480303665

van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society; Newcastle upon Tyne, 12*(2), 197–208.

Decisions made by AI versus transparency: Who wins in healthcare?

ANASTASIYA KISELEVA

This paper explores how the "black-box" nature of AI conflicts with the transparency requirement in healthcare.

Keywords: artificial intelligence, automated decision-making, healthcare, informed consent, transparency

INTRODUCTION

Artificial intelligence ("AI")[1], fuelled by the increasing availability of healthcare data and rapid progress in analytics techniques, is bringing a paradigm shift to healthcare. "AI is getting increasingly sophisticated at doing what humans do but more efficiently, more quickly and at a lower cost."[2] By analysing data, AI can detect anomalies, make predictions, do real-time tracking, find correlations and thus make better and faster decisions. Due to constant self-learning and self-correcting mechanisms, AI provides greater accuracy.[3] Thus, AI systems can reduce the diagnostic and therapeutic errors that are inevitable in human clinical practice.[4] Analysing huge pools of data enables AI to find unexpected correlations and insights, which can be used to discover new therapeutic techniques, find causes of diseases and identify ways to prevent them. The benefits of AI use in healthcare are numerous and prominent.

In contrast, policy makers and scholars are still discovering the legal and ethical challenges of AI use in healthcare. This paper briefly explores one of the most crucial legal and ethical issues of AI use – transparency. This issue is a fundamental one due to the "black box" nature of AI. However, healthcare services can only be provided to patients if they provide their informed consent and if their personal healthcare data is processed

[1] The term "Artificial Intelligence" is used to combine many concepts such as neural networks, robots, machine learning and deep learning. Although the mentioned concepts are similar and overlap, they are not identical (the a more detailed analysis of the differences, see here: A. Kiseleva "What is artificial intelligence and why does it matter for Copyright", available at: https://www.4ipcouncil.com/application/files/6815/4876/6908/What_is_artificial_intelligence_and_why_does_it_matter_for_Copyright.pdf). While the differences between these concepts can highly influence on the rules to regulate them, the prior goal is to define the specific object to be analysed. In turn, this paper deals with the most promising subset of AI – deep machine learning as explained below.

[2] No Longer Science Fiction, AI and Robotics are Transforming Healthcare. PwC. Available at: https://www.pwc.com/gx/en/industries/healthcare/publications/ai-robotics-new-health/transforming-healthcare.html (accessed 18 April, 2019).

[3] Jiang F, Jiang Y, Zhi H, et al. Artificial Intelligence in Healthcare: Past, Present and Future. Stroke and Vascular Neurology 2017; 2

[4] See PwC, above fn. 2

DOI: 10.5281/zenodo.3297165

lawfully and with the necessary safeguards. When it comes to AI use, these requirements are difficult to fulfil. The present article explains the reasons for these difficulties.

AI: THE "BLACK-BOX" EFFECT AND AUTONOMY

The primary task for any research dealing with the challenges posed by AI is to understand its nature and main features. If we do not understand the nature of a threat, then we have already lost the fight against it. This paper deals with the most promising subset of AI – deep machine learning.

Machine learning in general is a current application of AI based on the idea that we should just give machines access to data and let them learn for themselves.[5] While standard machine learning is an advanced field of AI, deep machine learning is the most sophisticated subset of AI in existence today. Typical machine learning systems need to be told how to make an accurate prediction using the data they are fed. In contrast, deep learning is based on self-learning and on the use of artificial neural network algorithms to process information.

Although deep learning algorithms can be compared with human ways of thinking, humans do not fully understand and control how these algorithms work. "As long as learning algorithms are running, humans are not really controlling how they are combining and comparing data."[6] The general principle of deep machine learning can be described as "transforming inputs to outputs through a black box".[7] In other words, machine learning is a fast, automatic and not intuitively explanatory self-learning mechanism.[8] When AI constantly engages in self-learning, the possible output is difficult to predict and explain. The combination of these features means that humans have a minimal level of control and understanding at all the stages of AI decision-making. Hence, autonomy and the black-box effect are the main features of AI that create the challenges described below.

[5] Gautam Narula, 'Everyday Examples of Artificial Intelligence and Machine Learning' (TechEmergence, 22 July 2018) https://www.techemergence.com/everyday-examples-of-ai/ (accessed 18 April, 2019).

[6] Cary Coglianese and David Lehr, 'Regulating by Robot: Administrative Decision Making in the Machine-Learning Era' (2017). Faculty Scholarship.1734. https://scholarship.law.upenn.edu/faculty_scholarship/1734/ (accessed 18 April, 2019).

[7] Ibid

[8] Ibid

AI AND THE TRANSPARENCY REQUIREMENT IN HEALTHCARE

A lack of transparency is the main issue with AI use in healthcare.[9] The very nature of AI algorithms means we cannot explain and predict the outcome of AI decision-making. This feature of AI is in conflict with the basic requirements of healthcare. Specifically, informed consent is a must for medical treatment and any other intervention into health. The general rule has been established by the Council of Europe in Convention on Human Rights and Biomedicine №164 ("Biomedicine Convention"). Under Article 5 of the Biomedicine Convention, an intervention into health may only be carried out after the person concerned has given free and informed consent to it. Moreover, this person has to be given appropriate information beforehand as to the purpose and nature of the intervention as well as on its consequences and risks. However, this requirement is difficult to fulfil when AI is used. "Currently there are limited strategies to uncover why a decision was made by an AI."[10] For example, when AI is used to make decisions about personal treatment methods, the algorithms used and specific decisions made are difficult to explain due to AI's autonomy. Moreover, the convention requires complete and appropriate information about interventions into health to be given in advance, prior to intervening. However, due to the constant self-learning and black-box effect, the outcomes of AI use are difficult to predict.

Transparency is also required under personal data protection legislation. AI functioning is based on using a huge pool of data, which often includes personal data. Under the GDPR, health, biometric and genetic data constitute special categories of data due to their particularly sensitive nature. With respect to AI, the GDPR has already introduced some regulations on automated individual decision-making, including on profiling. Article 22 of the GDPR states that solely automated decision-making that has legal effects on data subjects or that significantly affects the data subject and that is based on data concerning health, biometrics or genetics is only allowed with the data subject's explicit consent or if it is necessary for the public interest. In that case, the data subject has to be provided with meaningful information about the logic involved as well as on the significance and the envisaged consequences of automated decision-making for the data subject. Again, these requirements point to the features of AI that are in conflict with the transparency requirement: AI's autonomy and "black box"effect. The importance of resolving these issues is explained in the following.

[9] Besides transparency, the use of AI in healthcare creates other legal and ethical challenges such as the determination of rules applicable for AI's testing and approval; the accountability of healthcare providers; the problem of defining subjects to be held liable for false diagnosis, malpractice and other negative consequences of AI use; and the issue of establishing rules for such liability. However, the transparency issue is the fundamental one due to the very nature of AI algorithms and the dependence of the mentioned issues on the lack of transparency.

[10] Rajeev Dutt. Why Artificial Intelligence in Healthcare is Harder Than You Would Think. InfoWorld. Available at: https://www.infoworld.com/article/3269197/artificial-intelligence/why-artificial-intelligence-in-health-care-is-harder-than-you-would-think.html (accessed 18 April, 2019).

WHY TRANSPARENCY SHOULD WIN

A lack of transparency can lead to a decline in trust. Trust generally can be defined as the inclination of human beings to believe that a form of direct or indirect interaction with another person, thing or system may be beneficial to them or at least not harm their interests.[11] In healthcare, trust is often a key indicator of the quality of clinician–patient relations.[12] Moreover, social trust in healthcare providers can give them organisational and other benefits, such as a reduction in transaction costs due to lower surveillance and monitoring and a general enhancement of efficiency.[13]

When it comes to AI, trust issues have two elements: preserving existing trust in general health care systems and increasing trust in the use of AI technologies. "Trust is an important precondition for the adoption of new technologies."[14] This statement is supported by the recently published "Ethics Guidelines for Trustworthy AI" ("Guidelines") prepared by the High-Level Group on AI ("AI HLEG").[15] "In a context of rapid technological change, it is essential that trust remains the bedrock of societies, communities, economies and sustainable development."[16] Thus, trustworthy AI is identified as the "foundational ambition, since human beings and communities will only be able to have confidence in the technology's development and its applications when a clear and comprehensive framework for achieving its trustworthiness is in place."[17]

In turn, one of the main *requirements* for realising trustworthy AI is transparency.[18] Transparency is closely linked to explicability, which is one of the *principles* of trustworthy AI. "This means that processes need to be transparent, the capabilities and purpose of AI systems openly communicated, and decisions – to the extent possible – explainable to those directly and indirectly affected. Without such information, a decision cannot be duly contested."[19] In healthcare it means that decisions made by AI should be explained to patients to the most reasonable extent possible. The crucial issue here is to find a level of explicability and transparency of AI use that does not destroy the motivation of healthcare stakeholders to implement AI in their daily practice.

[11] Vedder, A. H., Cuijpers, C. M. K. C., Vantsiouri, P., & Zuleta Ferrari, M. (2014). The Law as a 'Catalyst and Facilitator' for Trust in E-health: Challenges and Opportunities. Law, Innovation and Technology, 6(2), 147

[12] Michael Calnan, Rosemary Rowe. Trust Matters In Health Care. 1 August 2008. UK Higher Education OUP Humanities & Social Sciences Health & Social Welfare.

[13] Ibid

[14] See Vedder, above fn. 11

[15] AI HLEG is an independent expert group that was set up by the European Commission in June 2018

[16] Ethics guidelines for trustworthy AI prepared by the High-Level Group on AI set up by the European Commission, as of 8th of April, 2019. Available at: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai (accessed 18 April, 2019).

[17] Ibid

[18] Ibid

[19] Ibid

CONCLUSION

AI is a self-running engine for growth in health care[20] and has the potential to improve its quality, efficacy and safety. However, the use of AI challenges the transparency requirement in healthcare. The black-box effect of AI's algorithms means it is not possible for healthcare providers to duly explain the nature and possible outcomes of AI use to their patients when diagnosing and treating them. It conflicts with the requirement to provide informed consent to interventions into health and with the right of data subjects to be provided with meaningful information about the logic involved as well as about the significance and the envisaged consequences of automated decision-making. In turn, the lack of transparency can lead to decline in trust. When it comes to AI, trust issues have two elements: preserving existing trust in general health care systems and increasing trust in the use of AI technologies. To ensure the transparency and explicability of AI algorithms, the healthcare industry should be provided with the relevant rules for AI testing, implementation and application. The law can be an effective tool to preserve and generate the trust necessary to persuade people to start and keep using AI.[21] Legislation should thus provide rules that make it possible to keep all the benefits provided by AI and at the same time minimise any negative impact.

BIBLIOGRAPHY

Calnan, M., Rowe, R., Trust Matters In Health Care. 1 August 2008. UK Higher Education OUP Humanities &Social Sciences Health & Social Welfare

Coglianese, C. and Lehr, D. Regulating by Robot: Administrative Decision Mak- ing in the Machine-Learning Era (2017).

Collier, M., Fu, R., Yin, L., Christiansen, P., Artificial Intelligence. Health- care's New Nervous System. Accenture. Available at: https://www.accenture.com/ t20171215T032059Z__w__/ us-en/_acnmedia/PDF-49/Accenture-Health-Artificial-In- telligence.pdf

[20] Matt Collier, Richard Fu, Lucy Yin, Philip Christiansen. Artificial Intelligence. Healthcare's New Nervous System. Accenture. Available at: < https://www.accenture.com/_acnmedia/PDF-49/Accenture-Health-Artificial-Intelligence.pdf (accessed May 25, 2019).

[21] See Vedder, above fn. 11

Dutt, R., Why Artificial Intelligence in Healthcare is Harder Than You Would Think. InfoWorld. Available at: https://www.infoworld.com/article/3269197/artificial-intelligence/why-artificial-intelligence-in-health-care-is-harder-than-youwould-think.html

European Commission ethics guidelines for trustworthy AI prepared by the High-Level Group on AI set up by, as of 8th of April, 2019. Available at: https://ec.europa.eu/ digital-single-market/en/news/ethics-guidelines-trustworthy-ai

Jiang F., Jiang Y., Zhi H., et al. Artificial Intelligence in Healthcare: Past, Present and Future. Stroke and Vascular Neurology 2017;2

Kiseleva, A. What is artificial intelligence and why does it matter for Copyright. (January 2019). 4iP Council. Available at: https://www.4ipcouncil.com/application/files/6815/4876/6908/What_is_artificial_intelligence_and_why_does_it_matter_for_Copyright.pdf

Machine-Learning Era' (2017). Faculty Scholarship.1734. https://scholarship.law.upenn.edu/faculty_scholarship/1734/

Narula, G., 'Everyday Examples of Artificial Intelligence and Machine Learning' (TechEmergence, 22 July 2018) https://www.techemergence.com/everyday-exam- ples-of-ai/

No Longer Science Fiction, AI and Robotics are Transforming Healthcare. PwC. Available at: https://www.pwc.com/gx/en/industries/healthcare/publications/ai-robotics-new-health/transforming-healthcare.html

Vedder, A. H., Cuijpers, C. M. K. C., Vantsiouri, P., & Zuleta Ferrari, M. (2014). The Law as a 'Catalyst and Facilitator' for Trust in E-health: Challenges and Opportunities. Law, Innovation and Technology, 6(2), 147.

Markets for eHealth: Perspectives from innovators and entrepreneurs

IRMA KLÜNKER

The panel discussion indicated that the features of the German healthcare system pose obstacles to entrepreneurial innovation.

Keywords: business model, electronic health record, innovation, insurance company

INTRODUCTION

A study by the Organisation for Economic Co-operation and Development (OECD) found that Germany spends over 11% of its gross domestic product (GDP) on healthcare, with only the USA (17%) and Switzerland (12%) having a higher health expenditure as a share of GDP (2017, 135). Accordingly, there is an increasing need for innovation to reduce the burden of healthcare costs, especially for an aging population. Using eHealth could potentially reduce the cost of health expenditure in Germany by up to 12% (PWC 2017, 13). This makes eHealth an attractive market for entrepreneurs.

Hence, at the end of the conference's first day, the "Markets for eHealth: Perspectives from innovators and entrepreneurs" panel discussed innovation and digitalisation in Germany. The consensus between the panellists was that Germany is lagging behind in health sector digitisation. Or, as Janis Reinelt, chair of the panel and business developer at Aicura Medical, put it: "The German health system is still in the 80s and has a lot of homework to do".

DRIVERS OF INNOVATION

Different perspectives were presented at the panel on the potential drivers of this much-needed eHealth innovation in Germany.

Docdirekt, an app offering telemedical services, is a pioneer in telemedicine in Germany. This is not because no one has thought of offering telemedical services through an app before. But until one year ago, there was a ban on remote treatment within physicians' professional codes in Germany's federal states. Docdirekt, however, is an app by the association of statutory health insurance physicians in the federal state of Baden-Württemberg (KVBW). It was launched after the medical chamber of Baden-Württemberg became the first of the federal states to lift the ban on remote treatment for pilot projects approved by the medical chamber. Therefore, Docdirekt offers services only to patients

DOI: 10.5281/zenodo.3297185

with statutory insurance in Baden-Württemberg, as panellist Clemens Schricker, who is part of the project management team controlling Docdirekt within the KVBW, explained during the panel. The example of Docdirekt illustrates that driving innovation is much easier when navigating the complex German healthcare system as a statutory body under public law.

In contrast, Mr. Reinelt, a business developer at a startup, says he doesn't expect innovation from within the system; instead startups should revolutionise the German healthcare system. And indeed, the government is lagging behind in providing patients with what would be the main use case of eHealth, an electronic patient record.[1] Berlin startup Vivy has seen the opportunity and launched their app, an electronic health record, although it is not the same as the government-planned electronic patient record. While, in a health system with public and private actors that are heavily intertwined, innovation certainly needs to be pushed by the public sector, the pressure to innovate seems to be coming from private actors.

BUSINESS MODELS

Having said that, startups can only be drivers of innovation if they have a business model. Despite this, panellist Farina Schurzfeld, co-founder and CMO at Selfapy, a Berlin start-up offering online therapy programmes, said that they didn't have a business model at the beginning. But she explained that their first deal with a health insurance company was crucial for the startup. Similarly, panellist Yannick Schmid, business intelligence analyst at Vivy, said regarding the business model, which involves partnering with insurance companies: "I think there's hardly any other way in Germany". In fact, other startups in Germany, such as the diagnostic app Ada, are also partnering with insurance companies (TK 2018).

This is also because eHealth users in Germany expect their insurance company to pay for medical services, as Ms. Schurzfeld explained. Patients are only willing to pay for the service themselves when they are desperate for help and under such conditions, eHealth is not the best choice, she says regarding their online therapy programme.

A different way of financing an app was presented by Annika Mierke, who is responsible for the design of the disease management app MyMate&Me, which is available to affected children at the Charité Hospital. Given its rather small target group and the fact that it was not available in an app store, MyMate&Me was sponsored by pharmaceutical companies Novartis and Nordic.

[1] According to the E-Health-Gesetz, the electronic health card was supposed to be provided with the function of the electronic patient record by 1 January 2019. However, according to the Terminservice- und Versorgungsgesetz insurance companies are obliged to provide insured persons with an electronic patient record only before 2 January 2021.

The UK has a different healthcare system to Germany, which also means that Solutions4Health, a digital healthcare provider, has a different business model, as Stan Thompson, director of strategy at Solutions4Health, explained. While in Germany, there is an obligation to have health insurance and every person pays an insurance fee depending on what they earn, in the UK the National Health Service (NHS) is paid for by taxes. Therefore, Solutions4Health's business model does not depend on the number of insurance companies they partner with but on whether the NHS takes on Solutions4Health as a healthcare provider. Mr. Thompson says this makes the business model much more reliable. In Germany, it is hard for a startup to predict whether an insurance company might be willing to partner with them when pitching for funding, Ms. Schurzfeld agreed.

OBSTACLES TO INNOVATION

Startups also face other obstacles to innovation in Germany. The healthcare system is complicated, and historically evolving systems can present national barriers to market entry, even within the EU, making internationalisation harder. Hence, venture capitalists investing in German health startups are scarce, as Ms. Schurzfeld explained. And when they find an investor, the usual e-commerce startup rules do not apply, as Mr. Reinelt reminded attendees, referring to the high stakes in eHealth. "Move fast and break things" may not be a wise saying in a market where failure may be fatal or result in data relevant for a very long time being misused, he said.

While Germany was characterised as state-of-the-art by the panellists in terms of data protection, as entrepreneurs they criticised continuing ambiguities regarding the General Data Protection Regulation (GDPR). These ambiguities, the agreed, result in startups spending more money on legal advice relative to big players and therefore hinder innovation.

CONCLUSION

Therefore, the question arises of whether the German healthcare system, described as "a weird system, somewhere between public and private" by Mr. Reinelt, is inimical to innovation. The panel discussion showed that in eHealth there are high barriers to market entry and that insurance companies take an active role in shaping the market. In the future, it will be interesting to see whether patients feel pressure to share more data with insurance companies due to the rewards offered or simply due to imbalances in negotiation power and the growing societal expectation to share data in general. Any ensuing data protection questions, however, were not one of the main topics discussed by

the panellists. Although Germany is lagging behind in the digitalisation of the healthcare sector, time will tell whether the current discourse on data protection will make future eHealth applications more secure for patients in the long term. Until then, we may see further evidence of the benefits of eHealth and observe an exciting growing market, with an estimated market demand for telemedicine solutions in Germany of almost 3.5 billion euros (European Commission 2018, 74).

BIBLIOGRAPHY

European Commission. (2018). *Market study on telemedicine.* Retrieved from https://ec.europa.eu/health/sites/health/files/ehealth/docs/2018_provision_marketstudy_telemedicine_en.pdf (accessed June 12, 2019).

OECD. (2017). *Health at a glance.* Retrieved from https://www.oecd-ilibrary.org/docserver/health_glance-2017-en.pdf?expires=1559554767&id=id&accname=guest&checksum=23AE7691BB997A981D630CDA450EF313 (accessed June 3, 2019).

Pwc, Strategy &. Effizienzpotenziale durch eHealth. (2017). Retrieved from https://www.strategyand.pwc.com/media/file/Effizienzpotentiale-durch-eHealth.pdf (accessed June 3, 2019).

TK. *TK setzt auf künstliche Intelligenz für bessere Versorgung.* (2018). Retrieved from https://www.tk.de/presse/themen/digitale-gesundheit/kuenstliche-intelligenz/start-von-ada-2053188 (accessed June 11, 2019).

International perspectives on eHealth

NIKLAS TRINKHAUS

The panel discussion demonstrated that particularities of the German healthcare system hinder innovation in the eHealth market.

Keywords: data protection, eHealth policy, interoperability, universal health coverage

INTRODUCTION

The achievement of universal health coverage (UHC) is part of the 17 Sustainable Development Goals issued by the United Nations in 2015 (UN 2015). The World Health Organization has since declared that "it has become increasingly clear that UHC cannot be achieved without the support of eHealth" (WHO 2016). Ameera Hamid, operations manager at the African Centre for eHealth excellence (Acfee) reminded the audience of the "Futures of eHealth" conference that telehealth in particular could play a central role in increasing access to healthcare and could enable "service delivery in underserved communities".

The implementation of eHealth technologies and the underlying infrastructure is therefore essential for low- and middle-income countries. But even high-income countries that suffer from a high degree of population dispersion or a shortage of doctors and healthcare professionals – for instance, Australia or Germany – could greatly benefit from new technologies like telemedical services. Apart from the provision and improvement of healthcare services, digitalisation in the health sector also promises more effective, affordable and personalised medical treatment.

Hence, all around the world, governments, academics, IT specialists and healthcare professionals are working to make these promises of eHealth a reality. While in some cases the promised progress through eHealth is already evident[1], the "International perspectives on eHealth" panel showed the multiple challenges that accompany hopes of healthcare improvement through eHealth.

[1] As shown during the live demo of an Indian telemedicine application by Dr Sai Praveen Haranath on the first day of the "Futures of Telemedicine" conference.

DOI: 10.5281/zenodo.3297209

WE NEED TO TALK: PEOPLE AND DATA INTEROPERABILITY

All the panellists highlighted the importance of health data interoperability. While a lot of countries are still struggling to implement the infrastructure and standards within their own country's boundaries, Mr Fernando Portilla presented the advances of the RACSEL[2] network in various Latin American countries. RACSEL is successfully working to connect regions and exchange experiences to implement interoperable electronic health registers (EHR) and to find strategies to connect countries on a transnational level. Other regions may benefit from RACSEL's experience on how to share information and support document and eLearning systems on a transnational level.

In order to take advantage of the benefits of eHealth for public health, a far-reaching and well-organised eHealth policy is needed. Mr Jai Ganesh, member of the governing committee of the Asia eHealth Information Network (AeHIN), reminded participants of the complexity of the field of eHealth and the plurality of stakeholders who need to be included when it comes to planning and designing a national eHealth strategy/policy. For this reason, AeHIN supports countries by bringing together this variety of actors. "People Interoperability" is at the heart of AeHIN's convergence workshops, where internal actors like the ministries of health, healthcare professionals, public health units and academics meet external partners like other ministries (e.g. finance and IT), development partners and international organisations, non-governmental organisations (NGOs) and other experts in the field of digital health. This variety of perspectives is important to establish a sustainable eHealth strategy for each region and to identify current challenges.

PREVENTING THE ABUSE OF HEALTH DATA

As health data are the most sensitive data that may be gathered, the hardest challenge is to guarantee the security of such data. When it comes to data governance, a lot of improvement is still needed: according to Acfee Chair Sean Broomhead, in some African countries, sensitive health data has been stored outside of national boundaries, oftentimes in contravention of local laws. Similar problems exist regarding mHealth applications in the European Union; their privacy policies sometimes contradict the General Data Protection Regulation (GDPR)[3]. A further problem identified in the African context arises when health data is maintained and managed by a third party and the local government has no control over the data and its usage. Mr Broomhead added that, in some cases, health data was used

[2] Red Americana de Cooperacion sobre Salud Electronica (eng. American Network of Cooperation on electronic health).

[3] See Mulder (2019) in this publication.

to apply pressure on governments with financial problems. Data files were locked and the country was no longer able to access its own data, because it was held by a third party. Incidents like this show the importance of strict regulation when it comes to public-private partnerships in the field of eHealth. Additionally, an intensified discussion on data governance and data ownership is needed on a local and international level.

To identify if and where legal amendments are needed, it is important to understand the plurality of laws and regulations that affect digital health. Getting an overview of the legal frameworks that affect eHealth technologies was one of the central aims of the "Futures of Telemedicine" project at the Humboldt Institute for Internet and Society (HIIG). Identifying the various laws and regulations that have to be taken into account in the case of telemedical services is highly complex, as HIIG researcher Alina Wernick pointed out. It is not only necessary to consider transnational regulations like the GDPR and national laws (e.g. civil law and norms governing the national healthcare system); in the case of telemedicine in Germany, the question of professional secrecy is regulated by the 16 federal states. This complexity is not only problematic for healthcare professionals, patients and innovators but also for consumer protection agencies, who find it challenging to legally pursue the multiplicity of (above-mentioned) data protection violations.

So, while a lot of expectations have been invested in eHealth in general and telemedical services in particular, there is still a lack of clarity regarding liability and the processing of data (not only in cross-border contexts). Furthermore, regional, national and transnational law should be harmonised to provide legal clarity to healthcare professionals, innovators and patients.

Regarding the German context, Niklas Kramer, senior policy advisor at the German Federal Ministry of Health presented the current and upcoming efforts to move digital health forward in Germany and the European Union (e.g. the European Networks for Rare Diseases (Eurodis 2012)). Concerns regarding data protection might be stronger in Germany than in other contexts due to historical experiences and cultural perceptions of (state) surveillance and control. Mr Kramer therefore promised that the upcoming telematics infrastructure in Germany would be "the most secure infrastructure for all". So even if the discussion on data protection is sometimes criticised as slowing or even hindering innovation, it can successfully pressure governmental actors to invest in a secure IT architecture.

LESSONS LEARNED

The International Perspectives on eHealth panel demonstrated that hopes and expectations regarding eHealth are a unifying force around the globe. The achievement of *universal health coverage* should be a driving force for international cooperation and the

development of eHealth technologies and infrastructures. To achieve this goal, we can learn from the experiences of actors from many different regions of the world. To create a common basis, like common IT infrastructures, it is clearly important to exchange basic information and engage in knowledge transfer at an early stage. eLearning systems can have an integrating function, in that they enable sharing of expert knowledge and improve digital (health) literacy. Well organised networks are key to building bridges from diverse stakeholders' expectations and desires to the development and implementation of eHealth policies and technologies. To ensure the security of vulnerable health data, the discussion on data governance and ownership should be intensified on an international level to include concepts like purpose limitation and the possibility of introducing a global ban on the exploitation of health data.

Transnational networks like AeHIN, RACSEL and Acfee have shown that cooperation on a supranational level is possible and highly productive. By working together and using the potential of eHealth in the right manner, we can achieve universal health coverage. And once this succeeds, we may be able to talk about achieving the complete third Sustainable Development Goal: good health and well-being. For all.

BIBLIOGRAPHY

Eurodis. (2012). Rare Diseases Europe. https://www.eurordis.org/european-reference-networks. [Last accessed 04.06.2019].

Mulder T. (2019). Processing purposes of eHealth. In this publication.

UN (2015): Sustainable Development Goals. https://sustainabledevelopment.un.org/sdg3. (Last accessed 04.06.2019).

WHO (2016): Global diffusion of eHealth: making universal health coverage achievable. Report of the third global survey on eHealth. Geneva: World Health Organization; https://www.afro.who.int/publications/global-diffusion-ehealth-making-universal-health-coverage-achievable.[Last accessed 04.06.2019].

EHEALTH IN PRACTICE – CASE STUDIES

Unjani Nurses lead the way: How eHealth can improve access to healthcare in rural South Africa

DANIELA RUDNER, LYNDA TOUSSAINT AND NAO SIPULA

Unjani Clinics use electronic health records and teleconsultations to enhance patient care in rural South Africa.

Keywords: container clinic social franchise, health portal, nurse-led community-based healthcare, teleconsultations

INTRODUCTION

Unjani Clinics is a social franchising initiative that has created a primary healthcare container clinic network in underserved areas of the country in pursuit of Sustainable Development Goal 3, Good Health & Well-being. This is what Unjani nurses bring to their communities in low-income townships and informal settlements: equitable universal health cover that saves patients from exorbitant health expenditures. The nurses form part of the Unjani Clinic network, which was established in 2013 with the mission to provide accessible, affordable and quality preventive healthcare – partly enhanced by remote access to an oversight doctor. The network links a growing number of professional "nurse-preneurs" – 58 at present[1]. The nurses own and operate their own container clinics and offer exceptional customer service in the communities they originate from and where they are trusted. The initiative has to date created permanent employment for over 200 people and provided in excess of 807,000 consultations.

For South Africa today, the innovative Unjani Clinic model is highly relevant for various reasons: for one, it addresses the inequality that exists between private and public healthcare services in the country. Whilst private and public hospitals and clinics exist, there are too few to deal with the increasing healthcare burden; private healthcare is too expensive for the bulk of the population. With the support of trained assistants who perform repetitive healthcare tasks, nurses can offer a quality service on a low-cost, fixed-fee-for-service basis to low income earners, thereby providing an alternative to expensive private care or the over-burdened public health service. The Unjani Clinics model also strengthens the re-engineering of the South African Healthcare System by creating community based healthcare structures at the point of need. It uses eHealth to provide enhanced care to remotely located patients, offering a much needed "one stop" solution for quality primary healthcare.

[1] May 2019

DOI: 10.5281/zenodo.3297239

DEVELOPMENTAL AND OTHER CHALLENGES

South Africa has a very poor infrastructure and service delivery in remote rural areas and informal settlements. With the next hospital out of reach in terms of distance and resources, getting access to doctors is a challenge, even in urban areas. Nurses operating in these areas face healthcare demands that can easily transcend their scope of practice. This has created a need for solutions that connect patients, nurses and doctors to ensure direct and timely access to medical advice and care for chronic patients. Although nurses are highly qualified and experienced, it is difficult for any nurse to offer a consistent high quality service resulting in loyal clients who refer family and friends. This requires a well-organised work flow and an efficient way to access and manage patient data: paper files are impractical when operating from container clinics while data portability is important to allow patients to visit all clinics in the network. The need for data interoperability has also arisen due to Unjani's intention to become a service provider to the planned National Health Insurance system and to integrate its patient data with the National Health Database.

Many of Unjani's challenges such as "infrastructure & connectivity", "sustainability", "integration with national platform services" etc. concur with "the key challenges on the way towards a digital health ecosystem" (Stroetmann 2018, 13), suggesting that they could be elegantly solved with digital solutions. For the Unjani Network, it became clear that they required a reliable data management system that would offer good patient data security, portability and scalability.

HEALTH PORTAL AND TELE-CONSULTATIONS FOR ENHANCED HEALTHCARE

Health portal

The solution that Unjani implemented was a system called Health IQ2, now called WatIF Health Portal, a multi global award-winning platform consisting of a combination of an Android and web application with a single database deployed on Microsoft's database management system SQL server. The underlying software architecture is a client-server model combined with a web application. The advantage of this is that the data processing platform is independent of the client side to the greatest possible extent while leveraging the exponential power of cell phone capabilities in a continent where cell phone adoption is in excess of 90%. The web application was implemented to run on the server side with access to integrated disease management, monitoring and evaluation graphics that serve as reporting tools. The health portal requires only cell phone connectivity and solar power to connect the entire clinic network across the country and deliver the world's first cell-

phone-based patient electronic health record management system. It provides users with a shared single view of patient health records that is accessible in real time. The portal is designed as a health workforce multiplier by using information and communication technology (ICT) to incorporate assistants into mainstream clinical work for purposes such as recording vital signs for patients and capturing laboratory test results as well as personal and family histories. This information is processed through the WatIF health knowledge database to generate patient-specific, actionable clinical-decision support output statements. These are presented to the nurse in the form of a "clinical dashboard" that provides her with a graphical representation of the patient's health status, risk profile and progress.

The nurse also has the ability to register her chronic patients on the health portal, giving them access to their own essential electronic health records through a personal portable interactive medical application that is Android based. All patients registered on the health portal benefit from an in-app free voice call service to healthcare facilities as well as from text chat and regular in-app notifications and reminders for important schedule items and health news. The patient app comes with functionality that allows patients to produce a detailed, system-generated referral letter when visiting health facilities that are outside the Unjani Network of clinics. Patients have access to an emergency call system that sends an SMS and email to a registered ambulance/emergency service, providing a detailed summary of their health status as well as their GPS location. Unstable diabetic and hypertensive patients can be monitored from the comfort of their homes using Bluetooth-enabled glucose meters and blood pressure machines that enable them to share clinical information with the nurse/doctor in real-time from a remote location through their medical app.

Teleconsultations

Unjani started testing tablet-based teleconsultations in several of the remotely located clinics in 2018. The facility allows a nurse to electronically share the patient's health record, including medical images, with a doctor (with the patient's consent) and to contact the doctor electronically via in-app chat. There is no need for the patient to leave the Unjani Clinic premises. Having the nurse in the consulting room with the patient allows the doctor to "use the nurse as his/her hands". Any additional instructions by the doctor, such as additional tests, take place remotely on a shared single patient file. An added benefit is that the Unjani nurses all speak the local language of the area and can translate for the patient and doctor to ensure that there is understanding and accurate communication of the condition, treatment and health education. Through the remote consultation process, the doctor can confirm the diagnosis, agree a treatment regime with the nurse, and generate an electronic script for the treatment. If the nurse has the required

medication in the medicine room, she can provide the patient with the medication and begin treatment immediately; alternatively, the patient can take the script to the local pharmacy, and the nurse can monitor the patient through regular follow-ups. Thus, the teleconsultation adds significant value to the patient: it reduces the time it takes to either confirm a nurse's diagnosis or to refer a patient to a doctor in case the patient presents with a diagnosis outside the nurse's scope of practice.

RESPONSE TO DATA PROTECTION AND PRIVACY CONCERNS

Health information is sensitive. Patients have a right to privacy and data protection. Internationally, governments and industry have deployed efforts to create standards, such as the USA's Health Insurance Portability and Accountability Act (HIPAA)[2] of 1996, which deals with electronic exchange, privacy and security of health information (OCR 2003): The Health Level Seven (HL7) standard is a voluntary standard for healthcare applications that addresses the way information is exchanged electronically (Hettlinger 1994). Likewise, there is the Integrating the Healthcare Enterprise (IHE[3]) International profiles, which define interoperability standards in eHealth that improve the way systems share information (Bertini 2016). Townsend (2017) states that the EU Charter of Fundamental Rights has integrated data protection as a fundamental right next to the right of privacy. Following this international trend to protect privacy and data in healthcare, the South African Government has introduced various pieces of legislation[4], amongst them the Protection of Personal Information Act of 2013 (POPI). "The POPI Act has as its primary purpose the promotion and protection of personal information processed by private and public bodies, thereby giving effect and substance to the right of privacy contained in Section 14 of the Constitution" (Townsend 2017). However, the right to data protection and privacy needs to be weighed against the benefits of exchanging patient data to improve healthcare. The intent to have a fully integrated national shared electronic health record system, with interoperability at its core, drove the South African Government to publish The National Health Normative Standards Framework for Interoperability in eHealth (HNSF) in 2014 (Chowles 2014). The latter heavily relies on the above mentioned IHE profiles – and so does Unjani's patient management system. It also complies with the above mentioned HL7 standard, the HIPAA privacy rules and the POPI Act.

[2] Find more information on HIPAA on https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

[3] IHE International is an international standard development organisation that works with the International Standards Organization (ISO)

[4] Townsend (2017) lists the following pieces of legislation: The National Health Act No. 61 of 2003 and the National Health Amendment Act No. 12 of 2013; The Health Professions Council of South Africa's guidelines; The Electronic Communications and Transactions Act 25 of 2002 (ECT Act)

Access to Unjani's patient management system is permission based and user specific, with multiple background user authentication. It employs a system-generated, secure, unique user name and password that may be coupled with a biometric identification process. To enhance patient data security, high-level users are able to monitor and generate user login records and reports. Different healthcare workers only have access to their area of work or activity. Patient identity is verifiable through a photograph, national ID number and or fingerprint biometric identification. Patient files can only be accessed through such a verifiable identification process. The WatIF Health Portal makes use of the Microsoft Connected Health Platform, which is based on the extensive and agile principles of the Microsoft Connected Health Framework (Microsoft 2009) and provides features for optimising health ICT infrastructures. Data can be interchanged between two distinctly different ICT systems while maintaining patient data security and confidentiality; this is the way eHealth interoperability should be achieved as suggested by the American National Health Normative Standards Framework for inter-operability in eHealth.

CONCLUSION

Building a professional and growing clinic network that can even operate in remote rural areas and informal settlements has brought up a number of challenges, such as establishing and maintaining high quality service standards, having real-time access to patient data across the network, maintaining data integrity and patient confidentiality and finding a scalable system that also integrates with national platforms, etc. Many of Unjani's challenges could be solved by implementing eHealth applications such as a patient management system with a user-friendly health portal and the ability to do teleconsultations and share patient health data. Experienced doctors are now able to support more than one clinic from a remote location in real time, thus reducing the need for patients to travel long distances to a referral centre and offering improved clinical response turnaround times. The above-described gains for patients have to be weighed against the risk of patient data abuse or a wrong diagnosis. The latter cannot be completely excluded; the question is whether the risk of an incorrect medical decision in a nurse-doctor tele-consultation is in fact higher than in a face-to-face doctor consultation. With regards to the risk of data abuse, Unjani's WatIF Health system complies with international and South African data security protocols and privacy rules. By being compatible and interoperable with most existing software applications and data platforms, including the national health information system, Unjani has striven to strike the balance between offering enhanced patient care vs maintaining protection of patient information.

The question of whether South Africa's legislation and Unjani's measures are sufficient to protect privacy and patient data stands against the question of the alternative: in a remote rural setting, a teleconsultation with a doctor is likely to be the only way to get access to a doctor at all and could easily become a lifeline. The lack of alternatives renders the privacy question a "luxury" consideration. With eHealth, Unjani nurses are being empowered to offer services that go beyond the normal nursing scope of practice; this might be inconceivable in the developed world, but in South Africa it has the potential to dramatically improve South African primary healthcare, in particular in remote rural areas or informal settlements.

BIBLIOGRAPHY

Bertini, L. (2016). IHE and its role in South African eHealth.

Chowles, T. (2014). NDoH releases HNSF for Interoperability in eHealth. Retrieved from https://ehealthnews.co.za/ndoh-release-framework-for-interoperability-in-ehealth-gazette-2/

Hettinger BJ. (1994). Health Level Seven (HL7): standard for healthcare electronic data transmissions. Retrieved from https://www.ncbi.nlm.nih.gov/pubmed/8149297.

Microsoft (2009). Connected Health Framework Architecture and Design Blueprint. Part 3 – Technical Framework. Retrieved from Microsoft.com

Office for Civil Rights (OCR, 2003). Summary of the HIPAA Privacy Rules.

Stroetmann, K. (2018). Digital Health Ecosystem for African countries. A Guide for Public and Private Actors for establishing holistic Digital Health Ecosystems in Africa.

Townsend, B. A. (2017). Privacy and data protection in eHealth in Africa. Chapter 5: Privacy and data protection measures within South Africa.

Addressing data privacy in digital health: Discussion on policies, regulations and technical standards in India

MANISHA MANTRI, R. RAJAMENAKSHI AND GAUR SUNDER

Keywords: digital health, data privacy, India, policies, regulations, security standards

INTRODUCTION

Digitalising health records is a boon to patients and hospitals when maintaining and managing treatment and plans. Digitising health records begins with collecting patient details at various data collection points and recording these. The collection points can be hospital front desks, clinics, diagnostic centres and healthcare devices generating patient specific data. The collection points store this data in their data storage repositories for further processing and future use. With growing data repositories and advancing technology, the risk associated with the data is growing. With digital health data, care must be taken to ensure the security of the data and to protect the privacy and confidentiality of the patient. In a healthcare context, patient confidentiality and the protection of privacy is the foundation for the doctor-patient relationship. It is necessary to ensure secure transfer of interoperable health records while transferring health records across all health care providers for treatments.

This paper discusses aspects related to handling privacy and security concerns in digital healthcare in India.

OVERVIEW OF PRIVACY IN HEALTHCARE

A digitised health record, often called an electronic medical record (EMR)/electronic health record (EHR), is comprised of patient demographics and clinical and other treatment-related information in electronic format (Sinha, Sunder, Bendale, Mantri, & Dande, 2012). These details are personal to the patient and require maintaining privacy and confidentiality of the data while handling it. Privacy is an individual's right to control the collection, use and disclosure of her personal information. Preserving privacy in healthcare refers to the non-disclosure of the patient's electronic health data to unintended and unauthorised persons.

One of the benefits of digital health is that it allows a sharing of health information for continuity of care. This sharing in turn increases the risk to privacy. As part of the ethical imperative to "first, do no harm", healthcare providers are required to ensure the

DOI: 10.5281/zenodo.3297267

confidentiality of healthcare information, as sharing it could lead to very serious harm, regardless of whether it is a “sensitive” issue such as mental or sexual health.

Privacy can be maintained through appropriate policies, data handling processes and technical safeguards. In digital health, possible threats to privacy could be:

- Theft, loss, damage or destruction/modification of health records
- Compromised access to health record systems
- Violations of security and privacy policies

In general, the patient is the owner of her health records. The patient has the right to access her records, to know the access details and to change or revoke the consent provided earlier. Consent is one of the critical elements in ensuring the patient's data privacy and confidentiality. Consent is obtained for different purposes and includes permission to perform healthcare activities, information about why, what and how the health information is collected and permission for clinical trials (Singleton & Wadsworth, 2006). It also includes health data sharing for referrals and research. Each healthcare provider should manage and maintain consent and access policies from patients or their representatives.

In the present-day scenario, the patient has almost no access to their consolidated electronic healthcare records. A patient’s clinical, pathological and imaging records are scattered across many places as she obtains treatment from different specialists. This makes it difficult for the patient to access the records. Due to different applications, platforms and formats used as well as differences in data quality, interoperability, exchange and access, this may be even more complicated. The following are a broad list of challenges in securing privacy of the patients in digital health records:

- Managing individual participation rights
- Accountability and access management
- Data cycle management and storage
- Case management and legal aspects
- Holistic application of privacy policies across public and private sector healthcare providers
- Cross border data exchanges
- Regulatory model to control data
- Breach management, managing penalties and offences

In order to address the challenges, we group, the problems under two headings. The first can be managed and solved using policies and regulations provided by governments and the other using the IT and data management policies.

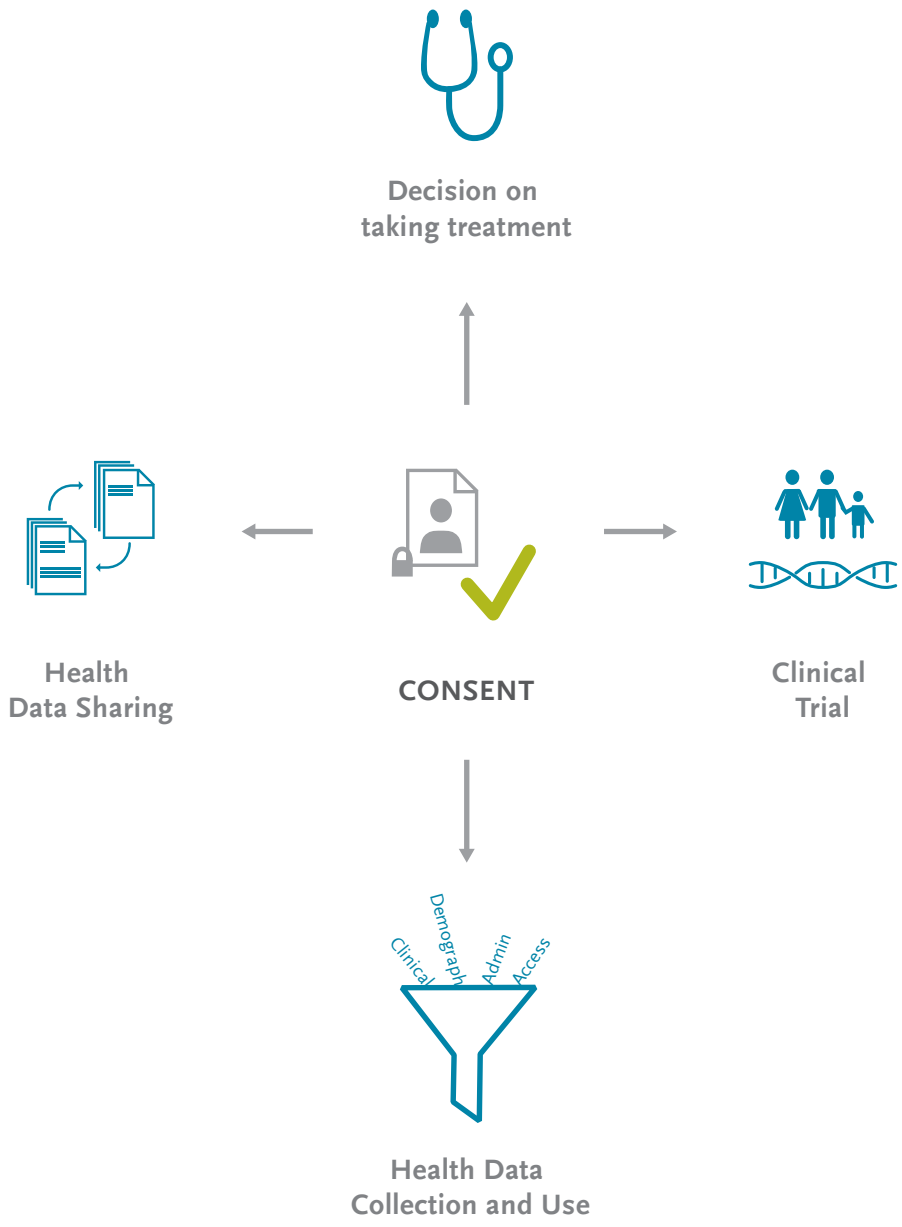
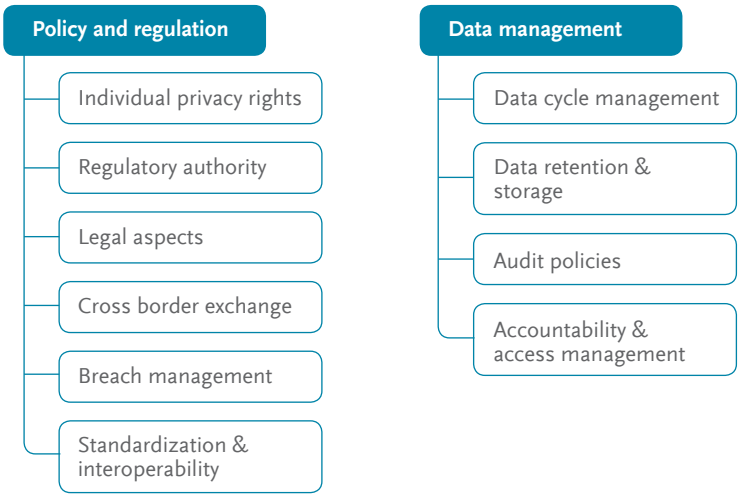


Figure 1. By author

Figure 2. Addressing privacy through policies, regulation and data management



DIGITAL HEALTH IN INDIA – A CASE STUDY

In a densely populated country like India, healthcare data lie in huge repositories scattered across different healthcare providers. This information is hugely important in providing healthcare to patients. Data is scattered across healthcare platforms, and doctors have no way to access a patient's complete electronic health records. Although healthcare data can be shared, there is a barrier due to privacy and security concerns when sharing. With the current legal framework, the collection, receipt, storage and handling and transfer of healthcare data in electronic form comes under the IT Data Protection Rules of 2011, a set of rules prescribed under the IT Act 2000 (IT Act 2008) and the Privacy and the Right to Information Act 2005 (Mishra, Parker, Nimgaonkar, & Deshpande 2008). The IT Act provides safeguards against certain of breaches in relation to data from computer systems. It contains provisions to prevent the unauthorised use of computers, computer systems and the data stored therein. It enforces personal liability for illegal or unauthorised use of computers, computer systems and data stored.

The Personal Data Protection Bill 2018 contains a comprehensive list of items that concerns individuals' privacy and aims to address these (MeitY 2018). The bill covers the processing of personal data by both public and private entities and administers processing of personal data:

- Within India
- By state, non-state or foreign entities within India.
- By data fiduciaries or data processors not present within India but having connection with any business in India

The bill is not applicable to anonymised data, but this does not extend to mere de-identification, a potentially reversible process where identifiers have been removed, masked or replaced with unique codes.

The bill covers the various aspects of processing personal data, including the obligations fiduciaries have regarding data processing, consent management, grounds for processing the data and especially sensitive personal data, data principal rights, and transparency and accountability measures, etc. Although the bill covers all aspects of data privacy, the principals may not suffice to ensuring patient privacy in healthcare scenario, where other aspects such as anonymisation, data retention, access control, etc. are crucial.

Healthcare in India is undergoing a transformation due to various initiatives in the area of digital health. The Indian government's two major initiatives towards addressing privacy in healthcare include:

(a) Electronic Health Record (EHR) Standards for India (recommendation set v2) for the interoperability and standardisation of EHR (and its derivative) systems in the country (EHRStandards, 2016)
(b) Digital Information Security in Healthcare Act (DISHA) (MoHFW 2017)

The next sections provide details on these government initiatives.

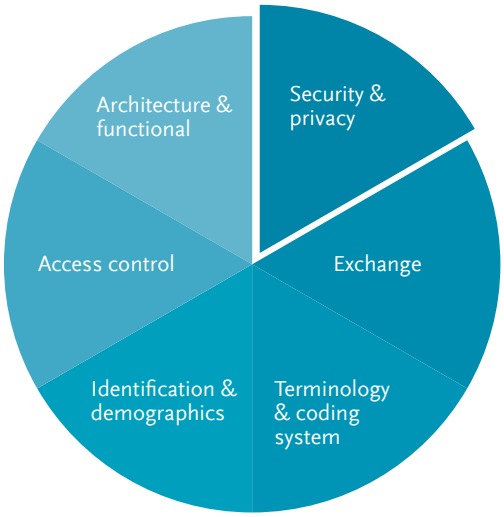
EHR STANDARDS FOR INDIA

The Government of India envisage a digital health ecosystem of interoperable electronic health record systems within the country. This can only be realised by having healthcare IT standards. The EHR Standards for India is one successful initiative enabling uniform standard practices, policies and mechanisms in healthcare applications. Given that there are a number of applications being deployed in public and private hospitals in India and that data is being collected and stored in digital form, the Ministry of Health and

Family Welfare came up with guidelines for the implementation and practice of health IT standards in 2016 (subsequent to the earlier notification in 2013).

The notification covers recommendations for various aspects of healthcare IT/ eHealth shown in Figure 3. The security and privacy requirements are discussed in detail in the next sub-section.

Figure 3. EHR Standards Coverage



PRIVACY AND SECURITY

The guideline covers important aspects of policies as well as process and technology standards that help to ensure the privacy and confidentiality of electronic health records. It defines the elements of health records that can be regarded as electronic protected health information (ePHI). ePHI is any protected health information (PHI) that is created, stored, transmitted or received electronically and would include passwords, financial information, physical, psychological and mental health condition, sexual orientation, medical records and history, and biometric information. The guideline refers to IT Act 2000 for deriving ePHI. The guideline specifies that the following policies be considered while handling electronic health records:

Data ownership

The ePHI, including health records, are owned by the patient; the care provider is the custodian of physical/electronic records.

A patient can demand a copy of her health records and care providers should provide all the required information in a stipulated time.

Data access and confidentiality

Patients have control over access to and disclosure of their individually identifiable health information. Explicit consent with access log need to be recorded for access to the information required for care. The patient can demand details of all the access log of her health records.

Denial of Information

The healthcare provider can deny the information to the patient or to any affected/interested party on the grounds of normal regulations and in cases where the information may harm the patient or others.

Disclosure of protected/sensitive information

There are various types of consents defined by the Medical Council of India (MCI) for treatment, payment, non-routine purpose (clinical trials), national priority activities (notifiable diseases), etc. Generally the consents are taken on documents and maintained separately. Being an integral part of health record, when taken consent should be reflected appropriately in electronic health records of the patient. The information can also be disclosed without the authorisation of the patient upon production of a court order, and totally anonymised health records can be shared by removing the patient's identifiable information.

Electronic health records preservation

It is evident that the fully consolidated electronic health records of individuals are a crucial source of information for prediction, medical research and many futuristic revolutions in health such as personalised medicine, genotype and phenotype-based diagnosis, prevention and treatment of diseases. The guideline recommends preserving health records for an individual's lifetime and suggests some mechanisms for managing the large data being generated.

These guidelines present a set of ISO/IEEE based standards that covers aspects of securing healthcare applications, protecting and preserving data privacy, encryption mechanisms, storage management, legal aspects, and interoperability standards. The ISO/TS 14441, ISO 22600, ISO 27789 and ISO/DIS 27799 standards provide extensive cov-

erage of security and privacy, privilege management and access control, audit trails and overall security requirements for health informatics systems. The guidelines also provide details on the retention policy and storage mechanisms for managing EHR applications.

DIGITAL INFORMATION SECURITY IN HEALTHCARE ACT (DISHA)

DISHA is the firm first step taken by the Indian government in the long journey to securing the healthcare data of patients in India. DISHA aims to be a piece of legislation focused on healthcare data privacy, confidentiality, security and standardisation. The primary objectives of DISHA are:

(a) Setting up a central and state-level digital health authority
(b) Enforcing privacy and security measures for digital health data, and
(c) Regulating the storage and exchange of electronic health data

Although the provisions of the IT Act with regard to data protection apply to any corporate that deals with the Sensitive Personal Data or Information (SPDI), the compliance requirements under the Data Protection Rules were largely limited to obtaining consent prior to collection or transfer, publishing a privacy policy, and maintaining "reasonable" security practices and procedures to protect SPDI. There are ISO standards that specify the set of requirements to preserve a person's privacy. In addition to data protection laws, there was a need for a regulator both at the central and the state level to enforce the rights and duties envisaged under the legislation.

Under DISHA, the government has proposed to set up a National Digital Health Authority (NDHA), which would be the key authority entrusted with formulating standards and operational guidelines and protocols for the generation, collection, storage, and transfer of digital health data. Similarly, at the state level, state digital health authorities will be responsible for ensuring that the requirements of DISHA are followed on the ground, at the institutional level.

DISHA also proposes the setting up of eHealth information exchanges – the backbone of interoperability and access – which would process and transmit data between clinical establishments. This will ensure the flow of data between entities.

DISHA defines a wide set of rights possessed by the owners of data (i.e. patients) and impose duties on the collectors, generators and processors of healthcare data. Maintaining privacy and confidentiality is the foremost responsibility of the stakeholders, and the owners must be informed of any data breach of their digital health data. DISHA also governs data breaches and non-compliance with requirements of DISHA. DISHA was put up for public comments in 2017 and is currently in consideration for implementation.

CONCLUSION

With the increasing focus on digital health, data sharing and potential confidentiality breaches are the key concern. Health IT is one of the top industries regarding privacy and security issues (ClearData 2017). With growing literacy rates and increased knowledge acquisition via the internet, patients are becoming more conscious in terms of handling their health records.

In such situations, a countrywide homogenisation of privacy and security policies and processes for managing electronic health records is vital. Policies and processes for paper-based health records would be applicable but not sufficient for EHRs. It is rational to recommend technology for process and policy management and technical standards for safeguarding of digital health records.

Initiatives in India towards digital health along with the emphasis on the much anticipated issues related to data privacy have been discussed in this paper. Privacy and confidentiality in digital health can be ensured by cohesively implementing policies, processes and technology.

ACKNOWLEDGEMENTS

The authors would like to acknowledge Ministry of Health & Family Welfare, Government of India for giving opportunity to work in the field of standardisation in healthcare IT through the National Resource Centre for EHR Standards (NRCeS) project (NRCeS, 2019).

BIBLIOGRAPHY

ClearData. (2017, November 30). *Security & privacy in the era of digital health.* Retrieved from Healthcare IT News: https://www.healthcareitnews.com/blog/security-privacy-era-digital-health

EHRStandards. (2016, December 30). Electronic Health Record (EHR) Standards for India. New Delhi, Delhi, India. Retrieved from https://mohfw.gov.in/sites/default/files/EMR-EHR_Standards_for_India_as_notified_by_MOHFW_2016.pdf

IT Act, 2. (2008). *Information Technology Act 2000 (Amended in 2008).* New Delhi: Govt. of India.

MeitY. (2018). *The Personal Data Protection Bill - 2018.* New Delhi: Ministry of Electronics and Information Technology, Govt. of India. Retrieved April 15, 2019, from https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

Mishra, N., Parker, L., Nimgaonkar, V., & Deshpande, S. (2008). Privacy and the Right to Information Act, 2005. *Indian Journal of Medical Ethics, 5*(4), 158-161.

MoHFW. (2017). *DRAFT Digital Information in Healthcare Security Act (DISHA).* New Delhi: Ministry of Health & Family Welfare. Retrieved from https://www.nhp.gov.in/NHPfiles/R_4179_1521627488625_0.pdf

NRCeS. (2019, April 02). *National Resource Centre for EHR Standards.* Retrieved from National Resource Centre for EHR Standards: www.nrces.in

Singleton, P., & Wadsworth, M. (2006). Consent for the use of personal medical data in research. *BMJ (Clinical research ed.),* 255–258.

Sinha, P. K., Sunder, G., Bendale, P., Mantri, M., & Dande, A. (2012). *Electronic Health Record: Standards, Coding Systems, Frameworks, and Infrastructures* (Vol. 9). IEEE Press, John Wiley & Sons, Inc.

Case study: An integrated solution using AI to detect diabetic retinopathy and prevent vision loss

ARUN SHROFF

Diabetic retinopathy (DR) is a serious eye disease that affects over 148 million people worldwide and can lead to vision impairment and vision loss if it is not detected and treated early enough. However, there are not enough specialists worldwide to screen everyone at risk. Artificial intelligence (AI) algorithms have been shown to be effective in screening for DR from retinal images. We present an integrated end-to-end solution for early detection of DR using artificial intelligence (AI) that is being deployed and tested in India. We present the problem, the objectives of the project and an overview of the solution as well as the challenges faced.

INTRODUCTION

Diabetic retinopathy (DR) is a serious eye disease caused by diabetes mellitus that can lead to impaired vision and blindness. According to the WHO, the number of people with diabetes worldwide has nearly quadrupled, from 108 million in 1980 to over 422 million people in 2014, and it is predicted to affect over 640 million people by 2040[1]. Studies suggest that 35% of people with diabetes, or 148 million people globally, have some form of DR. And an estimated 10% or 42 million have vision-threatening DR (VTDR), making it one of the leading causes of blindness among working-age adults worldwide[2]. The risk of vision loss can be greatly minimised if DR is detected and treated early enough. Early detection of DR requires periodic eye examinations and screenings by an ophthalmologist or a trained eye-care professional. However, many developing and low-income countries do not have the necessary specialists, resources or infrastructure to do so effectively.

In India, for example, there are over 72 million people with diabetes, of which an estimated 25 million are afflicted with DR and 7 million with VTDR. However, India only has 15,000 ophthalmologists for a nation of 1.3 billion people—or a mere 9 specialists per million. Kenya, with a population of 48 million, has less than 100 ophthalmologists, and Angola has less than 20 for 29 million people. In addition to the dire shortage of

[1] World Health Organization, WHO Global Report on Diabetes. http://www.who.int/mediacentre/factsheets/fs312/en/

[2] Yau JW, Rogers SL, Kawasaki R, Lamoureux EL, Kowalski JW, Bek T, et al. Global prevalence and major risk factors of diabetic retinopathy. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3322721/

DOI: 10.5281/zenodo.3297289

trained professionals, many of the affected people live in remote areas with little or no access to an eye care clinic or a screening centre[3].

Diabetic retinopathy has become a global health care challenge that urgently needs innovative solutions in order to prevent vision loss among millions of people at risk worldwide. The good news is that recent advances in artificial intelligence (AI) can help solve this problem by automating many of the tasks involved in screening and diagnosis.

CURRENT METHODS TO DETECT DR

A variety of techniques are currently used to detect and classify DR. These include direct and indirect ophthalmoscopy as well as colour fundus photography. Single field digital fundus photographs have been shown to be an effective and practical way to screen for DR[4]. In this approach, a digital photograph of the retina is captured using specialised equipment such as a slit-lamp and fundus camera. The image is then examined by an ophthalmologist, optometrist or a trained professional to detect abnormalities such as microaneurysms, exudates, haemorrhages, and macular edema to determine if DR is present and its severity and stage of progression.

In general, according to currently accepted standards, DR is classified into one of the following five categories: no apparent retinopathy, mild, non-proliferative diabetic retinopathy (NPDR), moderate NPDR, severe NPDR, and proliferative DR (PDR) and diabetic macular edema (DME)[5].

For the purposes of screening, DR can also be classified as either referable or non-referable. The referable category includes moderate, severe and proliferative DR (PDR), and referable DME, while non-referable DR includes no DR and mild DR. A referable diagnosis generally requires a follow-up examination by an ophthalmologist for further investigation and treatment.

USING DEEP LEARNING TO DETECT DR

In recent years, many AI systems using deep learning have been successful in image recognition and classification tasks. For example, in the ImageNet challenge, which required the identification of objects in 1000 categories, the best models achieve a classification error

[3] International Council of Ophthalmology. Number of Ophthalmologists in Practice and Training Worldwide. http://www.icoph.org/ophthalmologists-worldwide.html

[4] American Academy of Ophthalmology, Information Statement Screening for Diabetic Retinopathy, 2014 https://www.aao.org/clinical-statement/screening-diabetic-retinopathy

[5] Wilkinson CP, Ferris FL, Klein RE, Lee PP, Agardh CD, Davis M, Dills D, Kampik A, Pararajasegaram R, Verdaguer JT. Proposed international clinical diabetic retinopathy and diabetic macular edema disease severity scales. Ophthalmology. 2003; 110:1677–1682. https://www.ncbi.nlm.nih.gov/pubmed/13129861

rate of less than 5% – exceeding the best human accuracy levels[6].

Many of these models have now been adapted successfully for use in a variety of medical image diagnosis tasks such as melanoma, breast, lung cancer detection and diabetic retinopathy detection.

In particular, in 2016, a team at Google published the results of a study for detecting DR, in which it had worked with doctors in India and the US. The results show that their AI model's performance when detecting DR and grading its severity was on-par with that of ophthalmologists. Their model had a combined accuracy score of 0.95, which was slightly better than the median of the 8 ophthalmologists consulted, who had an accuracy of 91%[7]. More recently, IDx-DR, a company in the USA, released software that was approved by the FDA for detecting DR.[8] It therefore appears feasible to use AI to screen DR.

AI-based systems for detection of DR offer the following potential benefits:

- Bridging the shortage of healthcare professionals and providing access to screening where none exists.
- Increasing the overall efficiency and scalability of current screening methods.
- Providing earlier detection of DR, thereby preventing vision loss for millions.
- Decreasing overall healthcare costs via earlier interventions when it is easier and less expensive to treat these diseases.

While an AI model can tackle the routine screening required for DR, trained human experts still play a very essential role in detecting many other eye diseases, as well as in providing advice, counselling, care and treatment. Our aim should be to use AI and technology to augment and complement human expertise rather than to replace It.

In 2018, we undertook a project to use AI for early detection of DR in India. The project was proposed at the ITU/UN AI for Good summit in Geneva in May 2018.[9] The proposal was aligned with the objective of using AI to accelerate the achievement of the UN's Sustainable Development Goals (SDGs) in the area of health. It was also presented at the ITU/WHO Focus Group on AI for Health (FGAI4H) at Columbia University in New York City, in November 2018,[10] and the proposal was accepted as one of the first eight use cases of AI for health by the ITU/WHO.[11]

[6] IMAGENET. Large Scale Visual Recognition Challenge 2017 (ILSVRC2017). http://image-net.org/challenges/LSVRC/2017/

[7] Varun Gulshan, PhD1; Lily Peng, MD, PhD1; Marc Coram, PhD; et al. Development and Validation of a Deep Learning Algorithm for Detection of Diabetic Retinopathy in Retinal Fundus Photographs. https://jamanetwork.com/journals/jama/fullarticle/2588763

[8] FDA News Release,FDA permits marketing of artificial intelligence-based device to detect certain diabetes-related eye problems, https://www.fda.gov/newsevents/newsroom/pressannouncements/ucm604357.htm

[9] Arun Shroff, Presentation at AI for Good Summit, AI for Primary Care and Service Delivery, May 2018, Geneva, https://www.itu.int/en/ITU-T/AI/2018/Pages/programme.aspx

[10] Arun Shroff, Presentation at ITU/WHO Focus Group on AI for Health, Columbia University, NY Nov 2018, https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20181114/Pages/programme.aspx

[11] ITU News, Artificial Intelligence for Health: ITU and WHO accept 8 new use cases, https://news.itu.int/artificial-intelligence-health-new-use-cases/

OVERVIEW OF SOLUTION

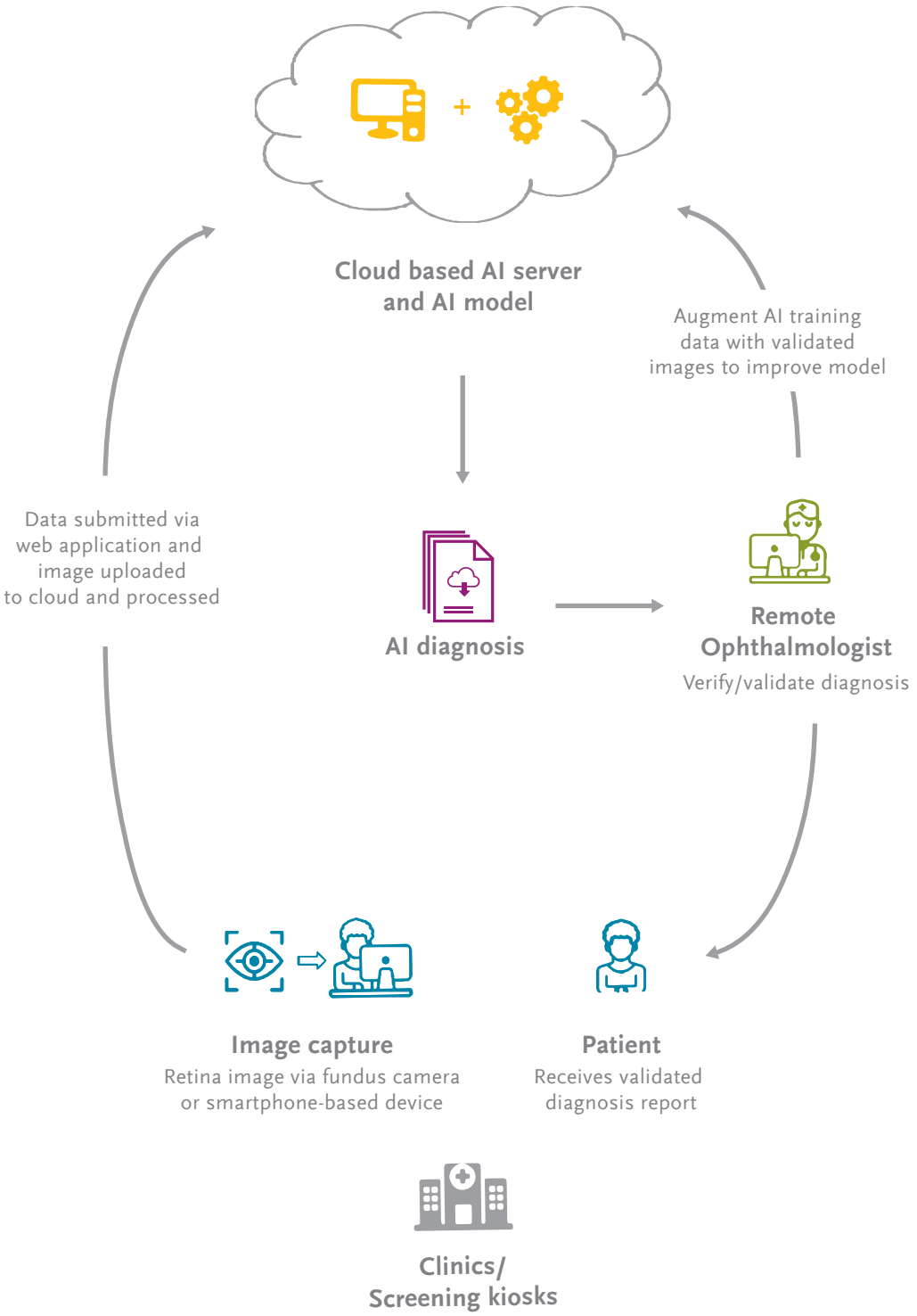


Figure 1. By author

SOLUTION OVERVIEW

An overview of the solution and its major components is as follows:

- The patient's retinal images are captured via fundus cameras at local screening centres or clinics and are uploaded via the web to a cloud-based server for further processing. A low-cost device that can be attached to a mobile phone for image capture of the retina is also being proposed for remote areas where no clinical facilities exist.
- A cloud-based web application for patient registration and data entry, image capture and uploading, integration with the AI model, remote diagnosis by trained specialists, and patient reporting, messaging and notification.
- Automated DR detection: The AI model runs on a remote server and automatically processes and classifies the image as gradable or not, and, if gradable, whether it is referable DR or not. It also provides information on the probability (or confidence level) of the classification.
- Remote diagnosis: Eye-care professionals can login remotely to the web application to review and validate the AI diagnosis, add notes and provide referral to a specialist as well as follow-up and treatment options. The system design will also incorporate the ability to fine-tune the AI algorithm based on corrections of diagnosis errors by the specialists.
- Integrated administrative, reporting and messaging for patient communication, system performance reports, and overall statistics.

IMPLEMENTATION AND TRIALS

We partnered with a leading teleophthalmology company in India, with over 275 screening centres in 22 states that screens over 25,000 patients a month for DR. It has a national network of ophthalmologists who perform the screening and diagnosis of DR remotely via a cloud-based application.

The creation of an AI model requires a sufficiently large dataset of images labelled with the actual diagnosis classifications previously obtained from human experts. The labelled data is then used to train an AI model using supervised learning. The model uses a convolutional neural network (CNN), and the training process fine tunes the weights of the network to minimise the error between the predicted classification and the true one. A part of the dataset, called the validation data, is not used for training, but used to validate the performance of the AI model on unseen data.

We started by first creating a dataset of approximately 90,000 images from our teleophthalmology partner. These images had been graded by licensed ophthalmologists and fell into one of the following categories: non-gradable, no retinopathy, mild NPDR,

moderate NPDR, severe NPDR and PDR, along with presence or absence of DME. The non-gradable category implied a low-quality image that could not be graded and assigned a diagnosis. All images were obtained with appropriate informed consent and anonymised prior to use in training.

For the purposes of the first phase of this project, we limited the scope to determining if the DR was referable or not. Therefore, the images were regrouped as:

i) Non-gradable
ii) Non-referable DR – which included no retinopathy and mild NPDR and
iii) Referable DR – which included moderate NPDR, severe NPDR, PDR and DME.

Approximately 80% of the dataset was used for training the model and 20% used for validation or testing of the model's performance.

The model was trained until it reached 92% accuracy on the validation dataset. The sensitivity of the model at the end of training was 92% and the specificity was 93%. Sensitivity refers to the proportion of positive (referable DR) cases that the model identifies correctly and specificity refers to the proportion of negative (non-referable DR) cases that the model identifies correctly.[12]

The AI model is currently being further tested and validated with real data while it undergoes field testing. The level of accuracy achieved by the model during testing is comparable to that achieved by ophthalmologists and is considered acceptable for screening for DR. In addition to internal validation, the AI model has also been submitted to the ITU/WHO's Focus Group on AI for Health, which has the goal of benchmarking AI for health algorithms and providing a neutral, independent assessment of performance.[13]

The technologies used can be briefly summarised as follows: it involves a ResNet-50 CNN architecture[14] built using Keras, Tensorflow and PyTorch software frameworks. The development was performed on a dedicated Intel server with an Nvidia GTX1080i GPU, and the web application was hosted on Amazon AWS infrastructure.

CHALLENGES FACED

In designing the system, we faced several challenges:

i) Data curation: the first challenge was to ensure that the data used for training the AI algorithm was clean. This is necessary to ensure that the trained model is accurate in making predictions on new images. Many large real-world datasets contain

[12] Wikipedia, Sensitivity and specificity, https://en.wikipedia.org/wiki/Sensitivity_and_specificity

[13] ITU Website, Focus Group on "Artificial Intelligence for Health, https://www.itu.int/en/ITU-T/focusgroups/ai4h/Pages/default.aspx

[14] Kaiming He, Xiangyu Zhang, Shaoqing Ren, Jian Sun, Deep Residual Learning for Image Recognition, https://arxiv.org/abs/1512.03385

invalid data and labels. For example, in our case, the data contained many anterior (outside) images of eyes. Images also varied in quality and included out-of-focus and low-quality images. We created a separate AI model to remove invalid and very low-quality images from the training dataset. This improved the overall accuracy, sensitivity and specificity of the AI model.

ii) Speed and scalability: design objectives for the AI system included fast prediction and scalability to hundreds of locations. By fine-tuning the model and parameters, we achieved a response time of less than a second on returning a prediction from the model. The system is hosted on Amazon Web Services (AWS) infrastructure, to ensure scalability when deployed across hundreds of locations.

iii) Data privacy, security & compliance: we designed the system to comply with Indian regulations, confidentiality and security by using informed consent, data privacy anonymisation and encryption, as proposed by the Digital Information Security in Healthcare Act (DISHA) and the Personal Data Protection Bill, 2018. India does not yet have formal regulations on using AI for health but requires all diagnostic reports to be reviewed and signed by a licensed doctor. Since the AI system will be used in assistive mode, all reports will be reviewed and validated by an ophthalmologist.

CURRENT STATUS AND DISCUSSION

The AI solution has achieved clinically acceptable levels of accuracy in initial testing and field trials in India and is ready for deployment on a larger scale. While regulatory approval for fully automated screening is still being sought, it will ultimately be used in an assistive mode as follows:

i) Improving screening throughput: currently 15% to 20% of images uploaded are non-gradable or invalid due to operator error. The AI system can instantly catch these errors and require the operator to capture a gradable image. This will reduce delays in diagnosis and improve overall throughput by 15% to 20%.

ii) Triage and prioritise screening: the AI system can identify higher risk cases and prioritise based on DR severity – with PDR, severe and moderate cases receiving immediate attention and priority screening. This will improve the overall level of care for those most at risk of vision loss.

iii) Quality assurance: in cases where the AI and ophthalmologist's diagnosis differ, the case can be automatically assigned to a second ophthalmologist for further review. This will improve overall accuracy and decrease errors.

We also plan to conduct field trials of the model in countries in Africa and the Far East, where there is an acute shortage of ophthalmologists. Future plans include obtaining FDA and EMA approvals for launch in the USA and Europe.

CONCLUSION

An integrated system using AI can be deployed at scale and be effective for early detection and screening of DR, a major cause of preventable blindness worldwide. AI based systems would be very useful in countries such as India and developing nations in Africa and elsewhere, which lack the professionals and infrastructure to screen everyone at risk of vision loss. Given that there are over 420 million people afflicted with diabetes worldwide and 148 million with DR and that the numbers are increasing each year, AI-powered systems will be critical to address the global healthcare challenge of DR and prevent vision loss for millions globally.

EHEALTH AND THE LAW: COMPARATIVE PERSPECTIVES

The demand for new legislation on eHealth in the EU

STEFAAN CALLENS

European input is needed for a better understanding of the role of certain joint controllers in healthcare and for the clinical assessment of digital health technologies. A data protection assessment in case of certain mergers in technology sectors is needed.

Keywords: clinical assessment of digital health technologies, joint controllers, mergers

INTRODUCTION

eHealth is popularly defined as "health services and information delivered through the Internet and related technologies".[1] eHealth comprises clinical information systems, telemedicine and home care, personalised health systems and services for remote patient monitoring, teleconsultation, telecare, telemedicine and teleradiology, integrated regional/national health information networks, distributed electronic health record systems and associated services such as e-prescriptions or e-referrals, and secondary usage of non-clinical systems (such as specialised systems for researchers, or support systems such as billing systems).[2] The concept of eHealth is continuously changing. Nowadays a lot of attention is being given to the digital health technologies (DHTs) i.e. apps, programs and software used in health and care systems, which may be standalone or combined with other products such as medical devices or diagnostic tests.[3]

Health systems have to focus not only on treatment but also on health promotion and disease prevention.[4] eHealth may provide the necessary means for delivering efficient and cost-effective care. By using digital solutions, citizens can actively engage in health promotion and self-management of chronic conditions.[5] To allow eHealth to improve patients' health status and to lead to a better health status and better care, more European rules, including European codes of conduct may be needed.

[1] European Group on Ethics in Science and New Technologies to the European Commission, Opinion no. 26: Ethics of information and communication technologies, (Publications Office of the European Union 2012) 33. See also: B. Kelly, 'E-health: ethical and data privacy challenges in the EU' (2011) Clinica 27; European Commission, eHealth Action Plan 2012-2020: Frequently Asked Questions, 2012; See also S. Callens,. "Ehealth" in European Health law, den Exter, A. (ed.), Maklu, 2017, 581-598.

[2] EHealth Taskforce, Accelerating the Development of the eHealth Market in Europe, (Office for Official Publications of the European Communities, 2007, 10.

[3] NICE, Evidence Standards Framework for Digital Health Technologies, 31

[4] European Commission, Communication on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, 25 April 2018, Brussels, 10

[5] Ibid.

DOI: 10.5281/zenodo.3297311

TRANSPARENCY REMAINS IMPORTANT

Joint controllers

The use of DHTs involves the participation of different actors, such as a cloud platform, a health institution or physician. This implies clear information on who is the processor and who is the controller of the data and/or whether there are joint controllers. Specific (European) codes of conduct regarding joint controllership in healthcare may help to ensure that actors in healthcare working with digital health technologies act in similar ways all over the EU.

Big data and AI

DHT often allows the fast processing of an enormous amount of totally different data. The use of big data and of AI in health and care requires transparency. Transparency in the field of artificial intelligence will imply that patients are informed of the intentions of developers and technology implementers of AI systems. According to the High Level Artificial Intelligence Group, it is necessary to clarify the method of programming the AI system or, if applicable, the method of training the algorithm.[6]

With regard to the use of AI, reflection on the suitability of some established rules on safety and on civil law questions on liability may also be needed.[7]

[6] High-level Expert Group on Artificial Intelligence Draft Ethics Guidelines for Trustworthy AI, (December 2018), 27. The UK Department for Health and Social Care, Code of conduct for data-driven health and care technology.

[7] European Commission, Artificial Intelligence for Europe, 2018, 15.

DHTS CLASSIFIED BY FUNCTION AND STRATIFIED INTO EVIDENCE TIERS

EVIDENCE TIER 1

System services
DHTs with no measurable patient outcomes but which provide services to the health and social care system.

EVIDENCE TIER 2

Inform
Provides information, resources or activities to the public, patients or clinicians. Includes information about a condition or general health and lifestyle.

Simple monitoring
Includes general health monitoring using fitness wearables and simple symptom diaries.

Communicate
Allows 2-way communication between citizens, patients or healthcare professionals.

EVIDENCE TIER 3A

Preventative behaviour change
Addresses public health issues: smoking, eating, alcohol, sexual health, sleeping and exercise.

Self-manage
Allows people to self-manage a specified condition. May include behaviour change techniques.

EVIDENCE TIER 3B

Treat
Provides treatment. Guides treatment.

Active monitoring
Tracking patient location, using wearables to measure, record and/or transmit data about a specified condition.

Calculate
A calculator that impacts on treatment, diagnosis or care.

Diagnose
Diagnoses a specified condition. Guides diagnoses.

Figure 1. Adapted from NICE, Evidence Standards Framework for Digital Health Technologies (March 2019, 7)

TOWARDS A EUROPEAN FRAMEWORK FOR THE CLINICAL ASSESSMENT OF DIGITAL HEALTH TECHNOLOGIES

Health technology assessments (HTAs) organised at the European level will be needed to guide member states in assessing new products. Health technology assessment is a multidisciplinary process that summarises information about the medical, social, economic and ethical issues related to the use of a health technology in a systematic, transparent, unbiased and robust manner[8]. Its aim is to inform the formulation of safe and effective health policies that are patient focused and seek to achieve best value[9]. HTAs can cover different aspects (domains) ranging from clinical domains (e.g. safety, clinical effectiveness) to non-clinical domains (e.g. economic, ethical, organisational)[10]. The proposal for a Regulation on Health Technology Assessment focuses on clinical assessments, which are typically based on global evidence (e.g. worldwide clinical trials for medicinal products and multi-national clinical trials for medical devices) compared with non-clinical assessments, which include domains that are often more sensitive to national/regional contexts[11]. According to the European Commission, the diversity and multitude of approaches to clinical assessments across the member states means that, due to their scale and effect, only action at EU level can eliminate the duplication of clinical assessment in the EU[12]. Where member states do carry out HTAs, there is, according to the proposal for a regulation, a requirement for mandatory use of joint clinical assessment reports.

With regard to the evidence to be analysed, the UK National Institute for Health and Care Excellence, known as NICE, published a document in March 2019 that describes standards for the evidence that should be available or developed for DHTs to demonstrate their value in a health and care system[13]. This evidence standards framework by NICE is intended to be used by technology developers when drawing up their evidence development plans and by decision makers who are considering whether to commission a DHT.[14] The framework may be used with DHTs that incorporate artificial intelligence using fixed algorithms but not for DHTs that incorporate artificial intelligence using adaptive algorithms (that is, algorithms which continually and automatically change)[15]. Separate standards will, according to NICE, apply to these DHTs. The NICE framework classifies the DHTs by function (see the Figure 1). The evidence level needed for each tier is proportionate to the potential risk to users presented by the DHTs in that tier[16].

[8] Proposal for a Regulation of the European Parliament and of the Council on health technology assessment and amending Directive 2011/24/EU, 1.

[9] Ibid.

[10] Ibid, 2.

[11] Ibid, 1.

[12] Ibid, 2.

[13] NICE, Evidence Standards Framework for digital health technologies, 2019.

[14] Ibid, 4.

[15] Ibid, 5.

[16] Ibid, 7.

THE NEED FOR MORE EUROPEAN INPUT REGARDING RESEARCH, CROSSBORDER CARE, REIMBURSEMENT AND MERGERS

The globalisation of healthcare actors and the need to do European research on complex diseases requires more harmonised rules on health data processing, especially given that the exchange of data between international or European eHealth actors will not just be used while treating patients in monitoring sessions – the data may also be processed for evaluation, research or statistical purposes. Article 89, 2 of the General Data Protection Regulation relates to the processing of (health) data for research purposes. However, this article leaves too much room for different legislation in the EU's member states. This may hinder the establishment of an emerging internal market of international quality review projects, epidemiological studies and clinical trials, etc. Moreover, the legislative differences between member states may be detrimental to the establishment of an internal market, especially in the context of the globalisation of healthcare. In other words, more European action is needed on this topic.

The commission has already pointed out that it intends to support the pooling of the EU's data resources and to facilitate their use for research and health policy[17]. National initiatives should be connected with European networks of scientific and clinical expertise, such as the International Consortium for Personalised Medicine, the European Reference Networks, the European Research Infrastructures, the Human Brain Project and other relevant initiatives[18]. According to the commission, this will help European research and industry remain at the forefront and will bring new personalised medical solutions to the market. The commission also believes that, by combining sequenced genomic data and other medical data, physicians and researchers can get a better picture of a disease in a particular individual and determine the most appropriate treatment for that individual. This should be based on a transparent system of governance, with the aim of linking national and regional banks of "-omics" data, biobanks and other registries across the EU[19].

The use of eHealth, including DHTs, will promote the shift from inpatient to outpatient treatment. The role of the hospital will change: a hospital will have to engage in much more monitoring of outpatients who are not physically admitted or not physically present in the hospital. Moreover, hospitals will be increasingly in touch with patients and healthcare professionals in other member states, whether the hospital acts as a reference centre or not. This will require clear European guidance on the exchange of information (and not only on ePrescriptions). This monitoring will imply that hospitals will have to organise their work and will have to draft stand-by arrangements, in cooperation

[17] European Commission, Communication on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, (25 April 2018), 8.

[18] Ibid, 8.

[19] Ibid, 8.

with many other healthcare professionals and hospitals given the increasing shortage of certain types of physicians in several member states (and the number of patients to be followed). Legislators will have to consider the need to follow up on monitoring activity and will have to facilitate this (cross-border) networking of health care professionals and hospitals. In this regard, Directive (EU) 2018/958 of 28 June 2018 on a proportionality test before adoption of new regulation of professions may play an important role.

Access to health care by using eHealth and/or DHTs will also imply the need to reimburse telemonitoring services. EU member states often still require the patient and the health professional to be present in the same place for a medical activity to be legally recognised and reimbursed. In many telemonitoring projects, this condition is not fulfilled. The question is whether the physical presence requirement, which represents an obstacle to the free movements of services, is a legitimate obstacle. Telemonitoring projects often end due to the lack of a financing structure. Although reimbursement is an issue to be dealt with by the member states, it might be helpful to develop clear European rules on the criteria, as was done in the past for the reimbursement of medicinal products by Directive 89/105/EC.

Applying big data and artificial intelligence in healthcare implies allowing speedy access to large quantities of health data, in conformity with data protection rules. However, attention must be paid to illegal refusal to uphold such data protection so as to avoid abuse of a dominant position and unfair competition. A statement by the European Data Protection Board (EDPB) on the data protection impacts of economic concentration argues that it is essential to assess the longer-term implications for the protection of economic, data protection and consumer rights whenever a significant merger is proposed, particularly in technology sectors of the economy.[20]

CONCLUSION

The European Union has published important documents on eHealth. Nevertheless, a continuous European input remains needed to promote the rights of European citizens, such as in the field of cross-border care, reimbursement and mergers in technology sectors.

[20] On the relation between data protection law and competition law, see I, Graef; M Husovec and N Purtova, "Data Portability and Data Control: Lessons for an Emerging Concept in EU Law", (2018), 19 German Law Journal 1359, 1388-1397.

BIBLIOGRAPHY

Callens, S, 'Ehealth' in *European Health law,* den Exter, A. (ed.), Maklu, 2017, 581-598.

European Group on Ethics in Science and New Technologies to the European Commission, *Opinion no. 26: Ethics of information and communication technologies,* (Publications Office of the European Union 2012) 33.

European Commission, *eHealth Action Plan 2012-2020: Frequently Asked Questions,* 2012.

European Commission, *Communication on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society,* 25 April 2018, Brussels.

European Commission, *Artificial Intelligence for Europe,* 2018.

EHealth Taskforce, *Accelerating the Development of the eHealth Market in Europe,* (Office for Official Publications of the European Communities, 2007.

Graef, I; Husovec, M and Purtova N., 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' , (2018) 19 German Law Journal 1357.

High-level Expert Group on Artificial Intelligence *Draft Ethics Guidelines for Trustworthy AI,* (December 2018).

Kelly, B; 'E-health: ethical and data privacy challenges in the EU' (2011) Clinica 27.

NICE, *Evidence Standards Framework for Digital Health Technologies.*

Proposal for a Regulation of the European Parliament and of the Council on health technology assessment and amending Directive 2011/24/EU

The UK Department for Health and Social Care, *Code of conduct for data-driven health and care technology.*

eHealth regulatory challenges in Russia

MIKHAIL ZHURAVLEV

The paper presents an overview of a new Russian law on eHealth and analyses legal issues concerning health information exchange and personal data processing in eHealth according to the Russian legislation.

Keywords: eHealth law, health information systems, personal data, Russian legislation

INTRODUCTION

During the last several years, eHealth has become a priority in governmental social policy in Russia. It is also linked to key pillars of the digital economy, which is the basis for current Russian economic policy.[1] Given the geographical and demographic specifics of the Russian Federation, telemedicine has great potential for remote Russian areas with poor medical infrastructure (where there is a lack of clinics or where access to health specialists is difficult, etc.). Besides the advantages for remote areas, there are more reasons to develop eHealth services in Russia. These include the potential of big data analysis of medical information, of the atomisation of healthcare management processes and of distant health monitoring to improve the quality of healthcare and make it more economically efficient.

Yet despite the existence of some successful eHealth projects in Russia,[2] it faces the same barriers to the widespread introduction of eHealth technologies as other countries: legal, ethical, financial and technological difficulties. Legal barriers are the most important ones as the regulatory environment sets the grounds for the eHealth industry.[3]

[1] In 2017, Russia approved a comprehensive long-term strategy for the development of information technologies "Digital Economy" similar to the EU Digital Single Market strategy. See Decree of the RF Government dated as of 28 July 2017 N 1632-p 'On approval of the programme "Digital Economy of the Russian Federation"' SZ RF, 7 August 2017, N 32, 5138.

[2] The largest Russian cities are the most successful ones in implementing information technologies in healthcare. For example, in Moscow since 2011 the Unified Medical Information-Analytical System (EMIAS) has been established. This system includes more than 600 public health institutions and provides tools for electronic interaction between patients, doctors and clinics. In particular, EMIAS provides electronic doctor appointments (including rescheduling and cancellation of appointments), maintenance of electronic medical records and writing electronic prescriptions. Each health worker has an electronic cabinet and ID card to log in to the system. In parallel, there is the electronic system of the Moscow Health Insurance Fund, which is designed to provide a personalised account of rendered medical services. Every patient has access to this system and may assist in monitoring the expenditure of the fund. Moscow medical organisations have possibility of issuing electronic certificates of temporary disability.

[3] A lot of Russian IT companies are interested in providing services in the field of eHealth. Now there are several services for electronic appointments with the doctor, online services helping patients to find the nearest clinics, etc. ("Yandex. Health", "DocDoc", etc.). The largest Russian telecom companies, MegaFon and MTS, also announced plans to offer telemedicine services. But the success of these services directly depends on the legal framework, which provides the regulatory environment and infrastructure for eHealth services.

DOI: 10.5281/zenodo.3297321

In 2016, the Russian government approved the "eHealth" programme[4]. The purpose of this programme is to increase the efficiency of medical assistance to citizens by introducing information technology. The programme was expected to accomplish the following:

- Monitoring electronic appointments;
- Transition of medical records into electronic form by not less than 50% of healthcare organisations by 2018 (80% by 2020);
- Implementation of at least 10 electronic services in the patient's "My health" personal electronic cabinet on the Uniform Portal of Public Services, which have to be available in 2018 to at least 14 million people and to 30 million people in 2020.

One of the strategy's first steps was the adoption of new federal legislation legitimising eHealth services and providing a legal framework for health information exchange.

In 2017, the so-called "Telemedicine Law"[5] was enacted in Russia, and it entered into force on 1 January, 2018. This law establishes the ability to issue electronic medical certificates, electronic prescriptions for medicines and medical devices and to give informed consent to medical interventions in electronic form; it also establishes the legal basis for health information systems.

However, this law has been viewed critically by the professional community (particularly by the IT companies interested promoting telemedicine services)[6], since the remote provision of medical care was not completely legalised by this law. It permits telemedicine consultations in order to prevent illness, collect and analyse patients' medical histories, evaluate the effectiveness of therapeutic and diagnostic measures and monitor patients' health, etc. Nevertheless, the initial diagnosis, the prescription of treatments and the remote monitoring of patients' health can be carried out only after a personal face-to-face visit with a physician. These limitations are the results of the conservative medical community's influence and information security concerns.

LEGISLATIVE FRAMEWORK FOR HEALTH DATA EXCHANGE

One of the most important challenges for the development of eHealth services consists in providing a free, secure and legitimate exchange of health data. The legal aspect of this issue entails two main problems: changing the legal framework for health information systems and revising the legal requirements for personal data protection given the

[4] See the Passport of priority project eHealth http://government.ru/media/files/9ES7jBWMiMRqONdJYVLPTyoVKYwgr4Fk.pdf (last accessed 2 March 2019).

[5] Federal Law of 29 July 2017 N 242-FZ 'On Amendments to Certain Legislative Acts of the Russian Federation on the Use of Information Technologies in the Field of Health Protection' SZ RF, 31 July 2017, N 31 (Part I), Art. 4791.

[6] '"Turn the wrong way": Why did the state refuse to listen to the IT industry on the issue of legalising telemedicine' (in Russian) https://vc.ru/p/legal-telemedicine, accessed 15 March 2019 ; 'Doctor on the wireline: what's wrong with telemedicine law' (in Russian) http://www.forbes.ru/biznes/358395-doktor-na-provode-chto-ne-tak-s-zakonom-o-telemedicine, accessed 15 March 2019.

specifics of eHealth technologies. Both problems need a comprehensive and consistent solution.

Health information system models have faced reform pressures in all the countries interested in promoting eHealth services. The main legislative development trends in this area include establishing the legality of electronic health records (EHR), centralising these records and empowering patients to manage their health records[7]. To comply with these trends, the regulatory framework for health information systems needs to be improved in a number of respects.

First, it is important to maintain the *integration and interoperability* of information systems. The structure of health information systems has to be open to public and private medical organisations at all levels (federal, regional, local), to research entities and to business associates. Of course, all participants in this structure have to act in line with publicly useful purposes and comply with information security requirements.

Second, it *requires the mobility and dynamism of data processed* in information systems. Data stored in health information systems should always be available for use by persons with a legitimate interest and should be regularly updated.

Third, it needs to *expand the applicability of information systems,* including cooperation with third parties offering innovative solutions in eHealth.

Fourth, there is *the patient's right to access and manage* personal electronic health records. Such access can be arranged through a personal electronic cabinet with a user-friendly and functional interface.

Several of these issues have to some extent been reflected in the Russian new legislation on telemedicine. Thus, in accordance with Article 91 "On the basics of healthcare in the Russian Federation"[8] the Unified State Information System in the Field of Health (EGISZ) operates in Russia. This unified system encompasses the information systems of public, municipal and private healthcare organisations. It can also incorporate the information systems of other governmental bodies and private entities that perform at least one of the specified functions (for example, providing information services for telemedicine sessions; statistical analysis, etc.).

Patients and doctors are identified via a single system of identification and authentication ("ESIA", a universal governmental system that is used to provide public services). However, it remains unclear whether it is possible to use alternative private platforms for identification.

Thus, in the Russian Federation significant steps have been taken to ensure interoperability of health information systems and the integration of telemedicine into the country's digital economy. However, further steps to ensure the interoperability of health

[7] See George Carlisle, Whitehouse Diane, Duquenoy Penny (Eds.). eHealth: Legal, Ethical and Governance Challenges. (Springer 2013) 40.

[8] The Federal Law dated as of 21 November 2011 N 323-FZ 'On the basics of healthcare in the Russian Federation', SZ RF, 28.11.2011, N 48, Art. 6724.

information systems involve the development of standards and specifications in the field of information exchange the establishment of such principles as openness, transparency, accessibility and a number of other interoperability principles that have received particular attention in countries in Europe and elsewhere.

ADAPTING RUSSIAN DATA PROTECTION LEGISLATION FOR EHEALTH

The importance of revising requirements for personal data protection has been recognised in many countries that have actively implemented eHealth technologies[9]. Even the GDPR does not provide final solutions[10]. Nevertheless, this issue has great relevance and needs thorough consideration.

The most problematic aspects of the current Russian legislation on personal data include the requirements for specific informed consent to processing personal data, the absence of dedicated rules for processing personal data in telemedicine and the collisions between legislation on personal data and provisions on medical secrets.

The issue of obtaining consent for personal data processing is perhaps the most pressing and controversial issue. One key aspect of it is the requirement of specificity. Moreover, since eHealth mostly deals with health information (a special category of personal data) the problem is reinforced by the necessity of obtaining written consent and of complying with many additional formalities.

Some authors have stated[11] that technologies involving distant personal data processing make the informed consent requirement a purely formal one and don't take into account a person's genuine will. As a result, such formalities just become barriers to implementation of new technologies instead of protecting individual autonomy. This idea is also applicable to eHealth.

Russian legislation prescribes the following requirements for receiving consent to health data processing: it should be given inwritten form[12]; the consent form should specify the list of personal data, the purposes and ways of processing, and all data processors;

[9] See Alexis Gilroy, Cristiana Spontoni, Katherine Llewellyn, Undine von Diemar. 'Data protection challenges for telemedicine in the EU and US' (2015) 2(8) E-Health Law & Policy 12

[10] See Victoria Hordern. 'Will the New EU Data Protection Regulation Facilitate Healthcare Innovation?' (2015) Chronicle of Data Protection. http://www.hldataprotection.com/2015/01/articles/international-eu-privacy/will-eu-data-protection-regulation-facilitate-healthcare-innovation/ (accessed 2 March 2019); Victoria Hordern. 'The Final GDPR Text and What It Will Mean for Health Data' (2016) Chronicle of Data Protection, http://www.hldataprotection.com/2016/01/articles/health-privacy-hipaa/the-final-gdpr-text-and-what-it-will-mean-for-health-data/ (accessed 2 March 2019).

[11] See e.g. Eugenio Mantovani & Paul Quinn. 'mHealth and data protection – the letter and the spirit of consent legal requirements' (2014) 28(2) International Review of Law, Computers &Technology. 222.

[12] European legislation stipulates that such consent should be explicit, but there is no obligatory requirement for written consent. See Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent – p. 25. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf (accessed 2 March 2019).

and it should also list details of a person's identity document and other requirements according to Paragraph 5 Art 9 of the Federal Law "On personal data".

Telemedicine technologies do not always imply the ability to determine in advance a specific list of personal data, the purposes for collecting that data and the ways of processing it[13]. It is particularly difficult to specify the exact purposes and ways of processing in medical research. Moreover, personal data in eHealth is dynamic in nature. This makes it necessary to obtain regular consent from patients to process their ever-changing health data.

The requirement to specify the identity document details seems quite excessive. First, this requirement is unlikely to guarantee informed consent. Second, the law requires specifying this sensitive information even in cases in which people do not want to communicate it to the data controller and the data controller does not need this information for the purposes of personal data processing.

Finally, specifying the list of entities and persons engaged into personal data processing (data processors) entails certain difficulties, since there are different actors involved in operating eHealth technologies. The list of these persons and entities may also change depending on various factors (purposes of processing, personnel replacements, introduction of new technologies and other possible changes in processing).

Russian legislation on personal data permits the processing of personal data without consent in a number of cases concerning medicine[14]. Certain types of telemedicine activities are likely to be consistent with exceptions already provided by legislation (for example, emergency medical assistance through telemedicine technologies). However, the essential part of eHealth, particularly its most innovative aspect (e.g. the internet of things for remote monitoring of health), is not covered by specific rules. There are even some obstacles when carrying out medical research using depersonalised (anonymised) personal data[15]. In contrast to the GDPR, Russian legislation still stipulates that statistical analysis and research with special categories of personal data (including health data) can

[13] This thesis is valid also for big data technologies in all areas, not only in medicine. See Savelyev A.I. 'The Issues of Implementing Legislation on Personal Data in the Era of Big Data.' (2015) 1 Pravo. Zhurnal Vysshey shkoly ekonomiki, 43–66 (in Russian).

14 These cases include the following: 1) processing of personal data is necessary to protect life, health or other vital interests of the data subject and obtaining consent is impossible; 2) processing of special categories of personal data is carried out for medical-preventive purposes, in order to establish diagnosis, render medical services if processing is carried out by a health professional obliged to keep medical secrets; 3) processing of special categories of personal data is carried out in accordance with the legislation on insurance; 4) processing of ordinary (not special category) personal data is carried out for statistical or other research purposes only after depersonalisation of personal data. There is no differentiation between anonymised and pseudonymised data in the Russian legislation.

15 Processing a large amount of personal data with modern technologies (namely big data technologies) cannot ensure genuine depersonalisation of personal data due to the de-anonymising potential of such technologies. A similar idea was expressed by EU Data Protection Working Party in the Opinion 4/2007 on the Concept of Personal Data, WP136 (2007), 18. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf (accessed 2 March /2019). About the impact of big data on the possibility of anonymisation see Jessica Santos. 'The Myth of Anonymization: Has Big Data Killed Anonymity?' (Kantar Health, 2015). http://www.kantarhealth.com/docs/white-papers/the-myth-of-anonymization-has-big-data-killed-anonymity-.pdf (accessed 2 March 2019).

only be carried out with the written consent of a data subject. Merely depersonalising the data is not enough.

In this regard, one of the possible solutions involves stipulating additional grounds for processing personal data without consent. These grounds can include such purposes as providing telemedicine services and carrying out scientific and statistical research with depersonalised health data.

It seems that approaches to consent should be differentiated depending on the public interest in processing certain personal data. When there is a public interest, the following approaches to consent can be used: 1) personal data can be processed without the consent of the data subject; 2) personal data can be processed without the consent of the data subject, unless the data subject has expressed a refusal to process his personal data ("opt out" model[16]).

In addition, it seems reasonable to unify the requirements covering consent to processing both ordinary and special categories of personal data. As noted earlier, written consent does not provide for higher protection of sensitive information but instead creates excessive obstacles to data exchange. In view of this, higher standards of security should be imposed on the processing of personal data for particular purposes and by particular means.

One more problematic issue for health data processing is the existence of personal data requirements and legislative provisions on medical secrets in parallel. In Russian legislation, there is no clear border line between these legal regimes. Thus, providers of eHealth services face a double legal burden and additional restrictions arising from the regulations on medical secrets. In the context of eHealth, this problem gains in importance as the range of entities engaged in data processing grow and the purposes and ways of processing become more complex. One possible solution involves establishing the priority of special legislation on medical confidentiality and the subsidiary application of the federal law "On Personal Data" to the processing of health information in cases that go beyond the scope of medical confidentiality[17].

[16] Russian legislation on personal data provides for the possibility of withdrawing consent to personal data processing. However, the law also stipulates that an operator may continue processing personal data if there are legal grounds for processing personal data without consent. Thus, Russian legislation does not include an opt-out model for obtaining consent to personal data processing.

[17] For example, Article 90 of GDPR lays down the legal framework for the implementation of a similar approach in member states' legislation.

CONCLUSIONS

The adoption of new eHealth legislation in the Russian Federation have laid the foundation for the electronic exchange of medical data. Currently there is a legal framework for health information systems that complies with the principles of integrity, interoperability, applicability and patient empowerment. The unified health information system provides an efficient environment for the development of eHealth in Russia.

At the same time, various legal challenges to eHealth remain relevant in Russia. For example, it is still impossible to diagnose and prescribe treatment based only on a telemedicine session. Overcoming this legal restriction entails addressing technological difficulties, patients' ethical concerns and the medical establishment's conservative beliefs.

The development of eHealth requires comprehensive legal support. In this regard we should not underestimate the importance of legal aspects concerning personal data protection in telemedicine. Legislative approaches to personal data protection directly influence public confidence in telemedicine and business readiness to invest in and offer innovative solutions in healthcare.

The issues of personal data protection in eHealth are not just specific eHealth issues. These issues also relate to fundamental problems with privacy law in a digital world. It is now an open question of whether the existing model of personal data protection will adapt to the new environment and survive or not. The answer will be revealed in the future, but it also depends on the efforts of the academic community, who will be active in recasting the role of traditional legal institutions in the digital era.

BIBLIOGRAPHY

Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf (accessed 02 March 2019).

Article 29 Data Protection Working Party. Opinion 4/2007 on the Concept of Personal Data, WP136 (2007) http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf (accessed 02 March 2019).

Carlisle, G; Whitehouse, D; Duquenoy P; (Eds), *eHealth: Legal, Ethical and Governance Challenges* (Springer 2013).

'Doctor on the wireline: what's wrong with telemedicine law' (in Russian) http://www.forbes.ru/biznes/358395-doktor-na-provode-chto-ne-tak-s-zakonom-o-telemedicine (last accessed 15/03/2019).

Gilroy, A; Spontoni, C; Llewellyn, K; von Diemar, U, 'Data protection challenges for telemedicine in the EU and US' (2015) 2(8) E-Health Law & Policy 12.

Hordern V; 'Will the New EU Data Protection Regulation Facilitate Healthcare Innovation?' (HL Chronicle of Data Protection 2015). http://www.hldataprotection.com/2015/01/articles/international-eu-privacy/will-eu-data-protection-regulation-facilitate-healthcare-innovation/ (accessed 02 March 2019).

Hordern V, 'The Final GDPR Text and What It Will Mean for Health Data// Chronicle of Data Protection' (HL Chronicle of Data Protection, 2016). http://www.hldataprotection.com/2016/01/articles/health-privacy-hipaa/the-final-gdpr-text-and-what-it-will-mean-for-health-data/ (accessed 02 March 2019).

Mantovani, E; Quinn, P, 'mHealth and data protection – the letter and the spirit of consent legal requirements' (2014) 28(2) International Review of Law, Computers & Technology 222.

Savelyev A.I. 'The Issues of Implementing Legislation on Personal Data in the Era of Big Data'. (2015) 1 Pravo. Zhurnal Vysshey shkoly ekonomiki, 43 (in Russian).

Santos, J, 'The Myth of Anonymisation: Has Big Data Killed Anonymity?' (*Kantar Health* 2015). http://www.kantarhealth.com/docs/white-papers/the-myth-of-anonymization-has-big-data-killed-anonymity-.pdf (accessed 02 March 2019).

'Turn the wrong way': Why do the state refused listen to IT industry on the issue of le- galising telemedicine' (in Russian) https://vc.ru/p/legal-telemedicine (accessed 15 March 2019).

'The passport of priority project "eHealth"' http://government.ru/media/files/9ES7jBWMiMRqONdJYVLPTyoVKYwgr4Fk.pdf (last accessed 02 March 2019).

ACKNOWLEDGEMENT

The paper was prepared within the framework of the Basic Research Program at the National Research University Higher School of Economics (HSE) and supported within the framework of a subsidy by the Russian Academic Excellence Project '5-100'.

Secondary use of clinical trial data in the Italian legal framework

PAOLA AURUCCI

Keywords: clinical data regulation, GDPR, health data, Italian law, secondary use

INTRODUCTION

Thanks to the digital revolution, coupled with advances in computing power, medical research is becoming increasingly data intensive.[1] The sources of such data include real-world data (such as electronic health records and data from patient registries)[2] and data from social media and wearable devices as well as records pertaining to genomics, clinical trials and adverse drug reactions (ADRs) reported during both the pre- and post-authorisation phases. Advanced computational technologies that are used to analyse and link heterogeneous data sets and that extract hidden patterns, correlations and links of potential significance are categorised as big data analytics.[3] According to the European Medicine Agency (EMA),[4] the use of big data in medicines development and regulatory science will become a major trend in the coming years. Yet, whilst the possibilities of innovative research springing from large-scale reuse and linkage of health and genomic data continue to expand, developments in IT and the reutilisation of sensitive data have triggered ethical issues[5] and posed two main obstacles. The first of these is technical and hinges on the lack of harmonised data while the second has to do with respecting the fundamental right to data protection.[6] This is because the objective of big data analytics is to discover unforeseen connections between data points that cannot be accurately predicted prior to carrying out the research.[7] As a result, it seems impossible for the controller to respect the purpose

[1] Menno Moster, Annelien Bredenoord, Monique Biesaart and Johannes van Delden, 'Big Data in medical research and EU data protection law: challenges to the consent or anonymise approach' (2016) 24 European Journal of Human Genetics 956

[2] Giovanni Corrao, 'Building reliable evidence from real-world data: methods, cautiousness and recommendations' (2013) 10(3) Epidemiology Biostatistics and Public Health https://ebph.it/article/view/8981 (accessed 14 May 2019).

[3] Alessandro Mantelero, 'Regulating big data. The guideline of the Council of Europe in the context of the European data protection framework' (2017) 33 Computer Law & Security Review 584, 585.

[4] European Medicine Agency, 'Role of big data for evaluation and supervision of medicines in the EU' (2019) https://www.ema.europa.eu/en/news/role-big-data-evaluation-supervision-medicines-eu (accessed 9 May 2019).

[5] Luciano Floridi, Christoph Luetge, Ugo Pagallo, Burkhard Schafer, Peggy Valcke, Effy Vayena, Janet Addison, Nigel Hughes, Nathan Lea, Caroline Sage, Bart Vannieuwenhuyse, Dipak Kalra, 'Key Ethical Challenges in the European Medical Information Framework' (2018) Minds and Machines 1.

[6] Ugo Pagallo, 'The Legal Challenges of Big Data: Putting Secondary Rules First in the Field of EU Data Protection' (2017) 3(1) European Data Protection Law Review 36.

[7] Brent D Mittelstadt and Luciano Floridi, 'The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts' (2016) 22(2) Science and Engineering Ethic 303.

DOI: 10.5281/zenodo.3297335

limitation principle, which is of fundamental importance for the general application of data protection rules and for compliance with these rules. To this extent, the coming into effect of the Clinical Trial Regulation or CTR[8] and the application of the General Data Protection Regulation or GDPR[9] will bring significant innovation in relation to the procedures for re-using information contained in large databases for scientific research purposes. In order to reconcile the often-competing values of data protection and innovation, the GDPR carves out numerous derogations for "historical or scientific purposes"[10], allowing researchers to avoid restrictions on secondary uses of sensitive data (Article 5(1)(b), Recital 50).[11] However, the availability of these derogations – analysed in Section 1 of this article – depends on the "appropriate safeguards" being set up by the data controller. At the same time, a possible interpretation of Article 28 (2) of the CTR seems to give the controller the duty to obtain consent from the data subject to lawfully further process clinical data at the time of the request for informed consent for participation in the clinical trial. In this case, further processing means uses of clinical trial data "exclusively" for scientific purposes that go beyond the initial intended purposes of the trial, as described in the protocol. This interpretation seems to open the possibility of broad consent or dynamic consent to the use of patient data in other research outside a specific study, recognised by Recital 33 of the GDPR, which allows data subjects to consent to future use of their data in certain areas of scientific research. According to another interpretation, however, optional consent to the further use of clinical trial data is not the same consent referred to in the GDPR as one of the legal bases for the processing of personal data (the provision is in fact "without prejudice" to the GDPR) but is a consent derived from the CTR itself.[12] In other words, this consent has to be regarded as the free and voluntary expression of the willingness of the patient to allow the secondary use of his/her data and not as an instrument for data protection compliance. The former is an ethical and procedural safeguard, while the latter is a restrictive legal basis for data processing. Since the intersection between GDPR and the CTR, which apply simultaneously in the context of clinical trials, is not as clear as it could be, the European Commission

[8] Council Regulation (EC) 536/2014 of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC [2014] OJ L158/1.

[9] Council Regulation (EC) 679/2016 of 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) [2016] OJ L 119/1.

[10] Gauthier Chassang, 'The impact of the EU general data protection regulation on scientific research' (2017) 11 ecancermedicalscience https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5243137/pdf/can-11-709.pdf (accessed 14 May 2019).

[11] Gabe Maldoff, How GDPR changes the rules of research, (IAPP, 19 April 2016) https://iapp.org/news/a/how-gdpr-changes-the-rules-for-research/ (accessed 14 May 2019).

[12] Kristof Van Quathem 'Further use of clinical trial data. Consent should not be mandatory in all cases (Inside Privacy, 1 October 2018) https://www.insideprivacy.com/wp-content/uploads/sites/6/2018/10/Further-Use-of-Clinical-Trial-Data.pdf (accessed 14 May 2019).

requested the European Data Protection Board (or EDPB) to comment on a draft Q&A document on this recognised issue. The EDPB issued its opinion[13] in that respect, which shall be analysed in Section 3. However, the possible impact of the application of gndC-TR and GDPR on current and future observational studies based on the secondary use of clinical trial information is only now becoming clear since – in this field – member states can use extensive discretionary powers. For instance, Article 9(4) of the GDPR allows member states to introduce further safeguards with regard to the processing of genetic data, biometric data or data concerning health.[14] With this in mind, the last section of the paper restricts the focus of analysis to the Italian legal framework, which on this specific subject, is a real "Dedalus"[15] of different inputs and rules.[16] After analysing new features introduced by Legislative Decree no. 101/2018, which has recently amended the Italian Data Protection Code, and by the recent Advisory Opinion of the European Data Protection Board on the interplay between the CTR and the GDPR, the paper aims to show how controllers and processors in Italy could re-use clinical trial data and at the same time demonstrate compliance with both legal and ethical requirements.

FURTHER USE OF PERSONAL DATA FOR SCIENTIFIC RESEARCH PURPOSES IN THE GDPR

As seen in the previous paragraphs, over the past twenty-five years, medical research has become increasingly data intensive. In this context, informed consent – considered for years the best mechanism to ensure a sufficient level of control of data – is being challenged. Since data are constantly shared, aggregated and reused, it is increasingly hard to predict who will be accessing the data in the future, for which purposes and under which conditions. Therefore, consent cannot be truly specific at the time of data collection. It is often impractical to re-contact each individual data subject to obtain explicit consent on the new research purpose; moreover it is prohibitively expensive and could undermine the validity of outcomes. In Recital 33, the GDPR recognises the difficulty of predicting all possible specific research purposes at the time of data collection and seems to allow for broader consent in certain areas of scientific research and for participants to select those areas. However, in complex research involving big data analytics, even the notion

[13] European Data Protection Board Opinion 3/2019 of 23 January 2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art. 70.1.b))

[14] Cf Pagallo (n. 5) 40.

[15] In Greek mythology, Daedalus was a skilful craftsman which was imprisoned within Daedalus the labyrinth he created.

[16] Cinzia Piciocchi, Rossana Ducato, Lucia Martinelli, Silvia Perra, Marta Tomasi, Carla Zuddas and Deborah Mascalzoni 'Legal issues in governing genetic biobanks: the Italian framework as a case study for the implications for citizen's health through public-private initiatives' (2018) 9(2) Journlal Community Genet 177.

of broad consent becomes weak.[17] It is very hard to foresee all the areas of possible future research at the time of collection. Furthermore, research that implies the use of AI techniques like machine learning are hypothesis-generating rather than hypothesis-testing, which means that it is often impossible to accurately predict the area of research prior to using the data. For this reason, Recital 50 provides for the possibility of drawing on the original data subject's consent or another legal basis that has allowed the original collection when the purpose of the new processing (further processing or secondary use) is "compatible" with the purposes initially declared. The proposition goes even further, stating that further processing for scientific research should in any case be considered "compatible lawful processing". This language is reflected in Article 5(1)(b), which provides that further processing for archiving purposes in the public interest, scientific or historical research purposes shall not be considered incompatible with the initial purpose. This presumption of compatibility with the purposes announced at the time of collection is related to the exemption to the principle of "storage limitation", which allows personal data to be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest and for scientific or historical research purposes or statistical purposes. Both articles, however, specify that this presumption of compatibility with the initial purposes is not fully automatic; it requires a data controller and a data processor to implement appropriate safeguards designed to protect the data subject and to reduce risks in accordance with Article 89(1). Article 89(1) specifies that the purpose of those safeguards is to ensure that specific technical and organisational measures are in place in order to ensure respect for the principle of data minimisation. The use of "pseudonymisation" techniques allows the controller to ensure respect for the principle of data minimisation (where anonymisation contrasts with the purposes of the processing). Recital 29 specifies that when pseudonymisation is used to make "general analysis" legitimate it must be combined with additional security measures to reduce the risk of re-identification.[18]

SECONDARY USE OF CLINICAL TRIAL DATA ACCORDING TO OPINION 3/2019 OF THE EDPB

Going back to the main topic of this paper, the CTR, which was introduced more than two years before the GDPR, addresses the issue of secondary use of clinical trial data. In Article 28(2), it appears to require informed consent to lawfully process the data of the

[17] Effy Vayena and Alessandro Blasimme 'Health Research with Big Data: Time for Systemic Oversight' (2018) 46/1 The Journal of Law Medicine and Ethics 119.

[18] Luca Bolognini and Camilla Bistolfi, 'Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation (2017) 33(2) Computal Law Secure Rev 171.

clinical trial subject "outside the scope of the protocol", but only – and "exclusively" – for scientific purposes. However, as pointed out in the introduction, it was not clear how this would interact with the GDPR since the CTR did not actually address in detail how the privacy rights of trial participants must be protected. On the contrary, it consistently refers to the GDPR in this regard. More clarity was provided by the EDPB, which, in its opinion – despite the statements to the contrary by the European Commission (EC) - clarified that optional consent under Article 28.2 CTR is not consent based on the GDPR but is consent derived from the CTR itself. It is therefore not subject to the consent requirements set out in Article. 4.11 and 7 of the GDPR. Furthermore, it goes in a slightly different direction to the EC, which, in the draft Q&A, excluded the presumption of compatibility provided under Article 5(1)(b) in all circumstances and recognised the possibility that secondary research could be considered compatible with the initial purposes of processing when conducted in accordance with Article 89(1). However, the EDPB points out that ensuring valid legal grounds is not enough to lawfully further process clinical data. In any event, even when the presumption of compatibility is found to apply, The controller is not exempt from all the other obligations under the GDPR, national laws and CTR. Given the complexity of the topic, the EDPB has made a commitment to give a specific opinion on this issue in the future. In the meantime, the committee does not rule out the application of the presumption of compatibility in the area of clinical trials.

ITALIAN IMPLEMENTING LEGISLATION: PRIMARY AND SECONDARY USE OF SENSITIVE DATA FOR RESEARCH PURPOSES

Although the GDPR is intended to reduce inconsistencies in the implementation of data protection across the EU, it gives back power to EU Member States. In line with Article 9(4) of the GDPR, the recently reformed Italian Data Protection Code ("DPC"), as amended by Legislative Decree no. 101/2018, adds further conditions in order to lawfully process primary and secondary health-related data for scientific purposes without consent or information to data subjects. Focusing first on the primary use of clinical trial data in the Italian legal framework, Article 2 septies of the DPC provides that sensitive data can be processed if specific safeguard measures (including security measures, such as encryption and pseudonymisation) are implemented. It also requires the Italian Data Protection Authority (Garante) to establish such safeguards at least on a two-yearly basis. The Italian legislation also goes in a slightly different direction than the EDPB as it relies on consent as the proper legal basis to justify the primary use of sensitive data for research purposes.

Furthermore, the further processing of sensitive data is subject to particularly strict requirements. The heading of Article 110-bis "Third party data reuse for purposes of scientific research or for statistical purposes", provides for two different scenarios: first, when a third party carries out the further processing of data (which means that the data controller is different from the first one that collected/processed the data in the first place) and second, when such further processing is carried out by a scientific institute for research, hospitalisation and healthcare. In the first case, subjects' consent to the further processing of data is only unnecessary when informing the data subjects proves impossible or involves disproportionate effort. Furthermore, in order to lawfully process personal data for scientific research purposes without informing data subjects, it is mandatory for the third party to comply with the limitation and conditions laid down in a "future" general authorisation that will be provided by the Italian Data Protection Authority. On the other hand, Article 110-bis(4) specifies that the secondary use for research purposes of personal data originally collected for clinical activity – by either public or private scientific institute for research, hospitalisation and healthcare – does not have to be regarded as a "third party data reuse" due to the instrumental nature of the activity of healthcare provided by the aforementioned institutions with respect to research. In this case, in fact, the further processing for research purposes is not carried out by a third party but by the same controller who collected the data in the first place. In this case, the presumption of compatibility set out in Article 5(1)(b) – provided that it occurs in accordance with the provisions of Article 89 - should apply and, therefore, the reuse of data for scientific research does not require a new legal basis such as consent. According to Article 106 of the IDPC, the Garante will set out these safeguards in the deontological rules relating to the processing of personal data for statistical and scientific purposes – which controllers/processors must respect to ensure the lawfulness of the processing – and probably also in the biannual guidance required by Article 2 septies of the IDPC.

CONCLUSION

The Garante did not release any official statement on the timing for its future publication and implementation of the biannual guidance/specific authorisation establishing specific safeguard measures to process biometric, genetic and health-related data, which will provide more clarity on the requirements for further processing health data (including clinical trial data) for research purposes. However, the general authorisation referred to in Article 40 of the Italian data protection code – which is not among the institutions governed by the regulation – is to be maintained for a transitional period. The Garante, by means of a general resolution, shall identify the provisions contained in the general

authorisations currently in force, which are compliant with the GDPR and/or the new Italian Data Protection Code. In this regard, the Garante's draft resolution, issued on 13 December 2018 (subject to public consultation) identified the provisions of previous general authorisation that seem to be compatible with the GDPR. Therefore, the General Authorisation to Process Personal Data for Scientific Research Purposes and to the processing of genetic data are a good point of reference for understanding legal bases and safeguards. Furthermore, on 19 December, 2018 the Garante issued the Deontological Rules Relating to the Processing of Personal Data for Statistical and Scientific Purposes. At present, the relevant legal framework applying to processing data for medical research in Italy is a complex combination of DPC's provisions, deontological rules, and specific authorisations of the Garante. In consequence, it is not easy to understand the impact of the EDPB Opinion on present and future Italian legal scenarios. More indications and guidelines are expected to be issued by the Garante.

BIBLIOGRAPHY

Bolognini L and Bistolfi C, 'Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation (2017) 33(2) Computal Law Secure Rev 171.

Chassang G, 'The impact of the EU general data protection regulation on scientific research' (2017) 11 ecancermedicalscience https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5243137/pdf/can-11-709.pdf (accessed 14 May 2019).

Corrao G, 'Building reliable evidence from realworld data: methods, cautiousness and recommendations' (2013) 10(3) Epidemiology Biostatistics and Public Health https://ebph.it/article/view/8981 (accessed 14 May 2019)

Floridi L, Luetge C, Pagallo U et al. 'Key Ethical Challenges in the European Medical Information Framework' (2018) Minds and Machines 1.

Knoppers B 'International ethics harmonization and the global alliance for genomics and health' (2014) 6(2) Genome Med 13.

Maldoff G., How GDPR changes the rules of research, (IAPP, 19 April 2016) https://iapp.org/news/a/how-gdpr-changes-the-rules-for-research/ (accessed 14 May 2019).

Mantelero A, ‘Regulating big data. The guideline of the Councile of Europe in the context of the European data protection framework’ (2017) 33 Computer Law & Security Review 584, 585.

Mittelstadt B, Floridi L, ‘The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts’ (2016) 22(2) Science and Engineering Ethic 303.

Mostert M, Bredenoord A, Biesaart M and van Delden J, ‘Big Data in medical research and EU data protection law: challenges to the consent or anonymise approach’ (2016) 24 European Journal of Human Genetics 956.

Pagallo U, ‘The Legal Challenges of Big Data: Putting Secondary Rules First in the Field of EU Data Protection’ (2017) 3(1) European Data Protection Law Review 36.

Piciocchi, C., Ducato, R., Martinelli, L. et al., (2017), Legal issues in governing genetic biobanks: the Italian framework as a case study for the implications for citizen’s health through public-private initiatives. J Community Genet, pp 1–14, doi: https://doi.org/10.1007/s12687-017-0328-2.

Van Quathem K. ‘Further use of clinical trial data. Consent should not be mandatory in all cases (Inside Privacy, 1 October 2018) https://www.insideprivacy.com/wp-content/uploads/sites/6/2018/10/Further-Use-of-Clinical-Trial-Data.pdf (accessed 14 May 2019).

Vayena E and Alessandro B ‘Health Research with Big Data: Time for Systemic Oversight’ (2018) 46/1 The Journal of Law Medicine and Ethics 119.

"Insuring" prioritisation and parity: Comparing approaches to telemental health in the law

LAUREN TONTI

Focusing on reimbursement parity, this research compares laws governing telemental health care in France, Australia and the Netherlands.

Keywords: mental health, parity, telehealth, telemedicine

INTRODUCTION

Mental health is critical to the discussion of eHealth's future, as mental health concerns contribute to the global non-communicable disease epidemic. The effects of mental ill-health have consequences not only for individual health and wellness but also for society's wellbeing. Mental health conditions, including depression, anxiety and substance use, affect one in six Europeans and one in five Americans.[1, 2] The European Commission has identified mental health as a priority agenda item, not only because of mental ill health's prevalence but also because of its costs. The Organisation for Economic Cooperation and Development (OECD) approximates the economic toll of mental health disorders in the European Union (EU) at €600 billion, a sum reflecting the steep costs of care, social benefits and loss of productivity.[3] Mental health also carries high human costs; in 2015 alone, at least 84,000 EU citizens died from mental health-related causes.[4]

Today, telemental health technologies offer the potential to promote prevention and purvey quality care. When discussing the practice of telemental health, this paper refers to psychological or psychiatric services delivered via telecommunication technologies.[5] Using video conferencing, computer programs and smartphone applications, mental health professionals can consult with and prescribe medication to patients, thus meeting the high demand for care. Preliminary studies evidence successful telemental health treatment and

[1] OECD, 'Mental Health Problems Costing Europe Heavily' (OECD 2018) <http://www.oecd.org/health/mental-health-problems-costing-europe-heavily.htm> accessed 19 April 2019.

[2] Centers for Disease Control & Prevention, 'Learn About Mental Health' (2018). <https://www.cdc.gov/mentalhealth/learn/index.htm> accessed 19 April 2019.

[3] OECD, 'Mental Health Problems Costing Europe Heavily' (OECD 2018) <http://www.oecd.org/health/mental-health-problems-costing-europe-heavily.htm> accessed 19 April 2019.

[4] OECD, Health at a Glance: Europe 2018 : State of Health in the EU Cycle. (OECD Publishing 2018).

[5] American Psychological Association, 'Guidelines for the Practice of Telepsychology' <https://www.apa.org/practice/guidelines/telepsychology> accessed 19 April 2019.

DOI: 10.5281/zenodo.3297349

indicate the potential for future applications and implementation.[6, 7] A study of telemedical insurance claims in the United States reveals that, while telemedicine use generally has increased over time, the highest increases in telemedicine services from 2005–2017 were either for telemental health care or primary healthcare, with a high demand for such services coming from rural regions.[8] The nature of telemedical technology means it is well suited to mental and behavioural healthcare delivery, which infrequently requires physical examinations or biological sample collection. This, combined with clinical effectiveness, has encouraged providers to increasingly embrace telemental health as part of their practices.[9] Realising the potential and demand for such services, governments have begun authorising and supporting the use of telemental health. However, without access afforded by insurance coverage, patients may not benefit from the potential of telemental health practice.

The reimbursement status of telemental health in the legal order remains unclear. In the process of developing unique approaches to telehealth regulation, some nations have opted to regulate telemental health services broadly under a catch-all telemedicine policy, while others treat the services singularly as their own category of law. Using a comparative approach, this research explores laws governing telemental healthcare reimbursement practice in France, Australia and the Netherlands. Beyond cataloguing the defining features of telemental health laws, this research analyses laws governing insurance compensation for telemental health services, with a particular focus on reimbursement parity with traditional mental health services.

WHAT IS TELEMENTAL HEALTH PARITY?

Mental health treatment parity, the concept that insurers should reimburse mental health services no more or less favourably than they would services for any other physical health condition, is an important lens through which to view telemental health services. In this research, I take achieving telemental health parity to mean that health systems reimburse telemental health services at the same rate as standard mental health services.

[6] Donald Hilty and others, 'The Effectiveness of Telemental Health: A 2013 Review.' (2013) 19 Telemedicine journal and e-health : the official journal of the American Telemedicine Association 444 <http://www.ncbi.nlm.nih.gov/pubmed/23697504> accessed 19 April 2019.

[7] Donald Hilty and others, 'Telepsychiatry: Effective, Evidence-Based, and at a Tipping Point in Health Care Delivery?' (2015) 38 Psychiatric Clinics of North America 559 <http://www.ncbi.nlm.nih.gov/pubmed/26300039> accessed 19 April 2019.

[8] Michael Barnett and others, 'Trends in Telemedicine Use in a Large Commercially Insured Population, 2005-2017' (2018) 320 Journal of the American Medical Association 2147 <http://www.ncbi.nlm.nih.gov/pubmed/30480716> accessed 19 April 2019.

[9] Epstein Becker & Green, 'Telemental/Telebehavioral Health' <https://www.ebglaw.com/telemental-telebehavioral-health/> accessed 19 April 2019.

Debate exists over whether telehealth parity is the right policy choice in general. Parity incentivises telehealth growth by encouraging both provider and patient uptake; this is because making services financially accessible encourages their use.[10] If the diversity of reimbursable health services increases, this provides incentives for increased telehealth infrastructure. Studies have demonstrated that parity can drive utilisation and have revealed potential to disincentivise telehealth uptake in states without parity laws.[11] Critics of telehealth parity argue that providers should not reimburse telehealth services at the same rate as in-person care because of the costs savings that streamlined, remote services can generate.[12, 13] Proponents rebut that if telehealth reimbursement practices do not match in-person provision, projected cost savings will be lost, as providers will encourage in-person visits to generate lost revenue and have little incentive to invest in telehealth infrastructure.[14, 15]

REIMBURSING TELEMENTAL HEALTH: COMPARING THE LAW IN FRANCE, AUSTRALIA AND THE NETHERLANDS

This analysis consists of systematic comparative inquiry into the definition of telemental health, reimbursement parity practice and the distinct features of telehealth law in France, Australia and the Netherlands. Three key criteria guided the comparison country selection. First, all jurisdictions permit general telehealth practice. Second, each has a universal health coverage system. The third criterion narrows the countries to those that have made recent policy changes to telehealth and telemental health care delivery. The research included only public insurance schemes and sought to inquire only into mental health care pertaining to mild to moderate disorders treated by outpatient therapy.

Definitions

Each of the French, Australian and Dutch legal orders approach defining telemental health differently, if at all. While the French Public Health Code does not explicitly define telemental health practices, telemental health services could fall under the code's general definitions of telemedicine and teleconsultation. In France, telemedicine is "a form of

[10] Jillian Harvey and others, 'Utilization of Outpatient Telehealth Services in Parity and Nonparity States 2010–2015' (2019) 25 Telemedicine and e-Health 132 <https://www.liebertpub.com/doi/10.1089/tmj.2017.0265> accessed 19 April 2019.

[11] Ibid.

[12] Y. Tony Yang, 'Telehealth Parity Laws' [2016] Health Affairs <https://www.healthaffairs.org/do/10.1377/hpb20160815.244795/full/> accessed 19 April 2019.

[13] Ateev Mehrotra, 'Telemedicine: Promise vs Reality' (Executive Education at Harvard Medical School 2019) <https://executiveeducation.hms.harvard.edu/telemedicine-promise-vs-reality> accessed 19 April 2019.

[14] Y. Tony Yang, 'Telehealth Parity Laws' [2016] Health Affairs <https://www.healthaffairs.org/do/10.1377/hpb20160815.244795/full/> accessed 19 April 2019.

[15] Ateev Mehrotra, 'Telemedicine: Promise vs Reality' (Executive Education at Harvard Medical School 2019) <https://executiveeducation.hms.harvard.edu/telemedicine-promise-vs-reality> accessed 19 April 2019.

remote medical practice using information and communication technologies. It connects, among themselves or with a patient, one or more health professionals, including necessarily a medical professional and, where appropriate, other professionals providing care to the patient. …It makes it possible to establish a diagnosis, to ensure, for a patient at risk, preventive follow-up or post-therapeutic follow-up, to request a specialised opinion, to prepare a therapeutic decision, to prescribe products, to prescribe or to perform services or acts, or monitor the condition of patients[16]…" The French Public Health Code also elaborates and defines each of the telemedicine practices permitted in France, including teleconsultation, which "is intended to allow a medical professional to give a remote consultation to a patient[17]".

While the Australian legislation does not explicitly define telemental health, Australia's Medicare Benefits Schedule requires a reimbursable video consultation to have both a visual and audio link between the patient and the remote care provider. This formulation makes clear that email or other internet messaging does not qualify for reimbursement. Finally, while some generally accepted definitions of eHealth exist,[18, 19, 20] telemental health appears to have no operational definition in Dutch law.

Telemental health parity

Telemental health parity operates explicitly in France. French law specifically ensures parity, stating in legislation that teleconsultation will be compensated at the same rate as in-person visits.[21, 22] As the national health insurance system compensates both standard mental health and telemental health consultations at a rate of 70%[23], parity exists between the practices.[24, 25]

[16] Code de la santé publique - art. L6316-1.

[17] Ibid.

[18] Raad voor Volksgezondheid en Samenleving, 'Consumer EHealth' <https://www.raadrvs.nl/documenten/publications/2015/4/21/consumer-ehealth> accessed 19 April 2019.

[19] Nederlandse Zorgautoriteit, Beleidsregel huisartsenzorg en multidisciplinaire zorg 2019 - BR/REG-19133 < https://puc.overheid.nl/nza/doc/PUC_236497_22/1/#result_4>.

[20] GGZ Nederland (Dutch Association of Mental Health and Addiction Care), 'E-Mental Health in the Netherlands' <https://www.ggznederland.nl/uploads/assets/Factsheet%20e-mental%20health%20in%20the%20Netherlands%20def.pdf> accessed 19 April 2019.

[21] Securité Sociale l'Assurance Maladie, 'La Téléconsultation' (Securité Sociale l'Assurance Maladie, 2019) <https://www.ameli.fr/assure/remboursements/rembourse/telemedecine/teleconsultation> accessed 19 April 2019.

[22] Securité Sociale l'Assurance Maladie, 'Consultations En Métropole : Vos Remboursements' (Securité Sociale l'Assurance Maladie, 2019) <https://www.ameli.fr/assure/remboursements/rembourse/consultations/metropole> accessed 19 April 2019.

[23] Seventy percent is the applicable reimbursement rate, so long as the patient accesses services through coordinated care pathways or has otherwise declared a care provider.

[24] Securité Sociale l'Assurance Maladie, 'La Téléconsultation' (Securité Sociale l'Assurance Maladie, 2019) <https://www.ameli.fr/assure/remboursements/rembourse/telemedecine/teleconsultation> accessed 19 April 2019.

[25] Securité Sociale l'Assurance Maladie, 'Consultations En Métropole : Vos Remboursements' (Securité Sociale l'Assurance Maladie, 2019). <https://www.ameli.fr/assure/remboursements/rembourse/consultations/metropole> accessed 19 April 2019.

While Australia does not explicitly enshrine parity in the law as in France, the Australian system does demonstrate telemental health parity. The Medicare Benefits Office (MBO) states that "[u]nder the Better Access initiative, new items for Telehealth services will be available at the same rebate as the existing ten face-to-face eligible services for allied health providers.[26]" The tariffs indeed reflect this policy. For instance, MBO reimburses a video consultation of 30–40 minutes in length at a rate of 100%, a rate identical to traditional mental health appointments of the same length.

By integrating eHealth practices into ordinary care, the Netherlands appears to embody "implicit" parity. Parity provisions are not specifically stated in the law. Instead, the Dutch system has deemphasised the distinction between digital and standard care. Because the Netherlands also encourages the use of blended care, which is a mixture of in-person and internet-based interventions[27] in mental healthcare, health insurers may reimburse all kinds of eHealth and not just video consultation.[28] The Netherlands has also reclassified telephone and email communications as "short" consultations, instead of single billed items, for "the form in which the care is provided... is therefore no longer leading for invoicing, only the time actually spent on patient contact.[29]" This change evidences how telemental health is implicit in standard care and shows that the care provided is a higher priority than the medium of care delivery.

Distinct features

Unique features of each nations' telemental health laws are important to highlight. While some of these policies apply to telehealth practice broadly, they also apply to mental health. France's health code mandates specific knowledge requirements of telemedicine to engage in its practice, requiring that telemedical professionals like psychiatrists and psychologists have adequate skills and training to use the technology.[30]

Australia's Better Access programme's geographic restriction is chief among the parameters of telemental health care access. Better Access allows patients to access telehealth services from "convenient" locations, including their homes, so long as patients "are located in an eligible rural, remote or very remote location... and not within 15

[26] Australian Department of Health, 'Better Access Telehealth Initiative for Rural and Remote Patients Guidelines' (2019) <http://www.health.gov.au/internet/main/publishing.nsf/Content/7711F1B8AF63FD55CA2581B50006892D/$File/Better Access Telehealth_Guidelines.pdf> accessed 19 April 2019.

[27] GGZ Nederland (Dutch Association of Mental Health and Addiction Care), 'E-Mental Health in the Netherlands' <https://www.ggznederland.nl/uploads/assets/Factsheet%20e-mental%20health%20in%20the%20Netherlands%20def.pdf> accessed 19 April 2019.

[28] Raad voor Volksgezondheid en Samenleving, 'Consumer EHealth' <https://www.raadrvs.nl/documenten/publications/2015/4/21/consumer-ehealth> accessed 19 April 2019.

[29] Nederlandse Zorgautoriteit, Circulaire vaststelling beleidsregel huisartsenzorg en multidisciplinaire zorg - CI/18/17c <https://puc.overheid.nl/nza/doc/PUC_244606_22/1/>.

[30] Code de la santé publique - art. R6316-10.

kilometres by road from their treating professional.[31]" The patient must not be admitted to a hospital or emergency room at the time of consultation.[32]

A special feature of the Netherlands' health finance scheme is a device known as the "max-max tariff". Applicable to mental health care, this device allows providers and insurers to contractually agree to increase the maximum rates of health services by 10%[33]. Such a device incentivises the adoption of innovative practices like digital healthcare.

REIMBURSING TELEMENTAL HEALTH: CHALLENGES AND FUTURE CONSIDERATIONS

This comparison reveals the many similar and disparate ways in which nations have introduced and implemented telemental health into care systems. All systems here permit telehealth practice more generally, and within that, telemental health practice, whether explicitly or implicitly. In some states, telemental health is treated separately, while in others, like the Netherlands, telemental health is implicitly rolled into standard health practice.

Comparing nations' approaches to telemental health reveals four key challenges that countries encounter when confronting telemental health practice. First, defining the scope of practice is a surmountable challenge. This analysis reveals that there is no standardised definition of telemental health practice among nations. While some of the definitions capture some of the same aspects of telemental health, like the concept of live audio-visual transmission, neither the definitions nor nomenclature of telemental health practice is standard. France does define telemedicine and teleconsultation in a way that encompasses telemental health, but it is one of the only countries to enshrine these parameters into national law. Stakeholders may find it difficult to discuss policy when the scope is ill-defined. Laws should explicitly state that telemental health is specifically included in the umbrella of practice, as this will clarify the law for legal interpreters and demonstrate that mental health is a legislative priority.

Second, health systems must also consider the transition from targeted intervention to broad practice. While Australia's geographic restriction are an example of how governments can use telemental health restrictions as precision instruments to ensure priority populations receive mental healthcare access, policymakers may eventually seek to expand telemental options to broader populations. In such a transition, health systems must ensure a sufficient supply of qualified health professionals to meet demand.

[31] Australian Government Department of Health, 'Better Access to Mental Health Care: Fact Sheet for Patients' <http://www.health.gov.au/internet/main/publishing.nsf/Content/mental-ba-fact-pat> accessed 19 April 2019.

[32] Australian Government Department of Health, 'Better Access to Mental Health Care: Fact Sheet for Professionals' <http://www.health.gov.au/internet/main/publishing.nsf/Content/mental-ba-fact-prof> accessed 19 April 2019.

[33] Nederlandse Zorgautoriteit, 'Wat Is Het Max-Max Tarief?' <https://www.nza.nl/documenten/vragen-en-antwoorden/wat-is-het-max-max-tarief> accessed 19 April 2019.

Third, telemental health technologies must find their place within existing health system structures. Though these systems were not originally designed with these healthcare practices in mind, each nation has found its own way to incorporate the practices. Varying approaches to finding that place may be one reason for the unique approaches evident in the law today. Because telemental health practice is not a cure-all, but rather a complement to practice, telemental health's legal architecture must reflect its complementary nature. Leaving ample room for future innovation is also a challenge. Holland's max-max tariff provisions highlight the importance of dedicating space in the system to incorporate future innovations in telemental health care.

Finally, in the future, lawmakers must prioritise mental health care in a world replete with digital tools. Should systems treat telemental health the same as other services? Or should it be uniquely prioritised? Can health systems implicitly include it in their offerings? Are priority and parity at odds? This research thus far cannot unequivocally conclude that telemental health parity only exists when it is inscribed in the law. It shows that even if specific parity provisions do not exist, as in Australia or the Netherlands, we can still find evidence of equal treatment. Reimbursement, a symbol of prioritisation, does not always equate to parity. Non-concretised regulation may open the door to disparate compensation in the future. The Dutch approach, where the focus lies on the care provided rather than the medium, could provide a viable solution. But which of these approaches is "best" will only become clear after each policy generates a body of evidence over time.

CONCLUSION

Telemental health practices have the potential to address the developing non-communicable disease epidemic. France, Australia and the Netherlands have each uniquely adopted telemental health care in their benefits schemes. Prioritising treatment and parity in insurance law alone is unlikely to ensure complete uptake of mental health care[34], but it is a necessary component of the endeavour. The challenges lie in parsing out who telemental health services cover, what they cover and how health systems deliver that coverage. While this brief analysis is limited, it does shed light on the need to address eHealth's challenges with clarity and precision.

[34] Jeongyoung Park and others, 'Are State Telehealth Policies Associated With The Use Of Telehealth Services Among Underserved Populations?' (2018) 37 Health Affairs 2060 <http://www.healthaffairs.org/doi/10.1377/hlthaff.2018.05101> accessed 19 April 2019

BIBLIOGRAPHY

American Psychological Association, 'Guidelines for the Practice of Telepsychology' <https://www.apa.org/practice/guidelines/telepsychology> accessed 19 April 2019.

Ateev Mehrotra, 'Telemedicine: Promise vs Reality' (Executive Education at Harvard Medical School 2019) <https://executiveeducation.hms.harvard.edu/telemedicine-promise-vs-reality> accessed 19 April 2019.

Australian Department of Health, 'Better Access Telehealth Initiative for Rural and Remote Patients Guidelines' (2019) <https://www.health.gov.au/internet/main/publishing.nsf/Content/7711F1B8AF63FD55CA2581B50006892D/$File/Better%20Access%20Telehealth_Guidelines.pdf> accessed 19 April 2019.

Australian Government Department of Health, 'Better Access to Mental Health Care: Fact Sheet for Patients' <http://www.health.gov.au/internet/main/publishing.nsf/Content/mental-ba-fact-pat> accessed 19 April 2019.

Australian Government Department of Health, 'Better Access to Mental Health Care: Fact Sheet for Professionals' <http://www.health.gov.au/internet/main/publishing.nsf/Content/mental-ba-fact-prof> accessed 19 April 2019.

Centers for Disease Control & Prevention, 'Learn About Mental Health' (2018). <https://www.cdc.gov/mentalhealth/learn/index.htm> accessed 19 April 2019.

Code de la santé publique - art. L6316-1.

Code de la santé publique - art. R6316-10.

Donald Hilty and others, 'Telepsychiatry: Effective, Evidence-Based, and at a Tipping Point in Health Care Delivery?' (2015) 38 Psychiatric Clinics of North America 559 <http://www.ncbi.nlm.nih.gov/pubmed/26300039> accessed 19 April 2019.

Donald Hilty and others, 'The Effectiveness of Telemental Health: A 2013 Review.' (2013) 19 Telemedicine journal and e-health: the official journal of the American Telemedicine Association 444 <http://www.ncbi.nlm.nih.gov/pubmed/23697504> accessed 19 April 2019.

Epstein Becker & Green, 'Telemental / Telebehavioral Health' <https://www.ebglaw.com/telemental-telebehavioral-health/> accessed 19 April 2019.

GGZ Nederland (Dutch Association of Mental Health and Addiction Care), 'E-Mental Health in the Netherlands' <https://www.ggznederland.nl/uploads/assets/Factsheet%20e-mental%20health%20in%20the%20Netherlands%20def.pdf> accessed 19 April 2019.

Jeongyoung Park and others, 'Are State Telehealth Policies Associated With The Use Of Telehealth Services Among Underserved Populations?' (2018) 37 Health Affairs 2060 <http://www.healthaffairs.org/doi/10.1377/hlthaff.2018.05101> accessed 19 April 2019.

Jillian Harvey and others, 'Utilization of Outpatient Telehealth Services in Parity and Nonparity States 2010–2015' (2019) 25 Telemedicine and e-Health 132 <https://www.liebertpub.com/doi/10.1089/tmj.2017.0265> accessed 19 April 2019.

Michael Barnett and others, 'Trends in Telemedicine Use in a Large Commercially Insured Population, 2005-2017' (2018) 320 Journal of the American Medical Association 2147 <http://www.ncbi.nlm.nih.gov/pubmed/30480716> accessed 19 April 2019.

Nederlandse Zorgautoriteit, Beleidsregel huisartsenzorg en multidisciplinaire zorg 2019 - BR/REG-19133 <https://puc.overheid.nl/nza/doc/PUC_236497_22/1/#result_4>.

Nederlandse Zorgautoriteit, Circulaire vaststelling beleidsregel huisartsenzorg en multidisciplinaire zorg - CI/18/17c <https://puc.overheid.nl/nza/doc/PUC_244606_22/1/>.

Nederlandse Zorgautoriteit, 'Wat Is Het Max-Max Tarief?' <https://www.nza.nl/documenten/vragen-en-antwoorden/wat-is-het-max-max-tarief> accessed 19 April 2019.

OECD, 'Mental Health Problems Costing Europe Heavily' (OECD , 2018) <http://www.oecd.org/health/mental-health-problems-costing-europe-heavily.htm> accessed 19 April 2019.

OECD., Health at a Glance: Europe 2018: State of Health in the EU Cycle. (OECD Publishing 2018).

Raad voor Volksgezondheid en Samenleving, 'Consumer EHealth' <https://www.raadrvs.nl/documenten/publications/2015/4/21/consumer-ehealth> accessed 19 April 2019.

Securité Sociale l'Assurance Maladie, 'Consultations En Métropole: Vos Remboursements' (Securité Sociale l'Assurance Maladie, 2019) <https://www.ameli.fr/assure/remboursements/rembourse/consultations/metropole> accessed 19 April 2019.

Securité Sociale l'Assurance Maladie, 'La Téléconsultation' (Securité Sociale l'Assurance Maladie, 2019) <https://www.ameli.fr/assure/remboursements/rembourse/telemedecine/teleconsultation> accessed 19 April 2019.

Y. Tony Yang, 'Telehealth Parity Laws' [2016] Health Affairs <https://www.healthaffairs.org/do/10.1377/hpb20160815.244795/full/> accessed 19 April 2019.

Prohibitions on long distance treatment: Historical roots and continuities in limiting the use of electronic telemedicine

ALINA WERNICK AND IRMA KLÜNKER

Many jurisdictions restrict the treatment of patients at distance via telemedicine. The article reviews the origins and justifications behind the limitations.

Keywords: eHealth, health law, prohibition of long distance treatment, telemedicine

INTRODUCTION

One of the advantages of telemedicine is its capacity to overcome the physical distance between a patient and a physician. Telemedical ICT technology, such as live-video interaction, may enhance patients' access to a wide variety of healthcare services[1], especially in areas that suffer from the shortage of physicians. With the help of technology, doctors could remotely treat patients situated in rural areas, other states or countries. However, in many jurisdictions, the availability of direct-to-consumer telemedicine is subject to legal constraints, such as prohibitions or limitations on offering long-distance medical treatment.

The legal norms that limit the use of telemedicine have the most straightforward impact on its adoption. These norms may take the form of a straightforward prohibition on long-distance treatment or on its important elements, such as diagnosis.[2] The limitations may also be more subtle; for example, they may focus on setting qualifications for consultations or examinations of the patient or criteria for medicine prescriptions.[3] Although present in many jurisdictions, we found no systematic review on these legal rules or their background.[4] In order to gain an understanding of the interests at stake and justifications behind the limitations of the provision of telemedicine, we will review the

[1] WHO, Telemedicine. Opportunities and developments in Member States (Report on the second global survey on eHealth, 2010) 7-9.

[2] In Germany, the prohibition on long distance treatment is still in force in the federal states of Brandenburg and Mecklenburg-Vorpommern, § 7 (4) of their respective Berufsordnung; in Russia, Article 36.2 of the federal law of 29.07.2017 N 242-FZ "On Amendments to Certain Legislative Acts of the Russian Federation on the Use of Information Technologies in the Field of Health Protection" prohibits a diagnosis without a face-to-face visit of the patient, see also: Mikhail Zhuravlev, 'eHealth Regulatory Challenges in Russia' in this publication.

[3] On the federal level, see Ryan Height Online Pharmacy Consumer Protection Act, Pub L 110-425, § 2-3, 21 USC § 829 (e), § 831 (h) (2008) (Ryan Height Act of 2008). In addition, many US states require the telemedicine provider to establish a relationship with the patient before issuing prescriptions and limit the provision of certain substances at distance. See for example Ind Code § 25-1-9.5-7 and § 25-1-9.5-8 (2018)

[4] For existing research, see Kazuyuki Nakayasu and Chiaki Sato, 'Liability for Telemedicine' (2012) 3(1) International Journal of E-Health and Medical Communications 1, 3; Anca M. Cotet and Daniel K. Benjamin, 'Medical Regulation and Health Outcomes: The Effect of the Physician Examination Requirement' (2013) 22 Health Economics 393.

DOI: 10.5281/zenodo.3297377

historical background and recent legislative developments in the telemedicine legislation in the US and Germany. Both of the countries have federal political systems and limit the provision of telemedicine. However, in the US, the limitations were enacted as a reaction to the digitalisation of medical care[5], whereas in Germany, the prohibition of long-distance treatment has historical origins dating back to the nineteenth century.[6]

LIMITATIONS ON TELEMEDICINE IN THE US

In the US, the Ryan Haight Online Pharmacy Consumer Protection Act of 2008 was enacted to tame online prescriptions of controlled substances[7] and the unlawful use of such substances by making them conditional on the performance of an in-person examination and regulating the registration of online pharmacies.[8] The act was motivated by a desire to prevent drug abuse by adolescents and was named after a young overdose victim.[9] Telemedicine-based prescriptions of controlled substances were permitted under seven very narrow exceptions.[10]

On the state level, telemedicine is not prohibited in the US. However, the regulations on online prescriptions vary dramatically between states.[11] Beyond the Ryan Haight Act of 2008, many states have additional, often stricter regulations on the prescriptions of controlled substances.[12] In addition, many states also make prescriptions of non-controlled substances conditional on the pre-existence of a physician-patient relationship. Some state laws explicitly specify that such relationship may be established via telemedicine.[13] As an alternative approach to legal drafting, some states permit the establishment of the relationship via telemedicine when it aligns with relevant standards of care.[14] Occasionally, the states impose further conditions, such as requiring live, real-time com-

[5] Ryan Height Act of 2008; see Anca M. Cotet and Daniel K. Benjamin (n 4) 407; the Russian limitations on the provision of telemedicine were also enacted as a reaction to modern ICT technology, see Mikhail Zhuravlev (n 2).

[6] In Japan, the principle of face to face examination also dates back to the Medical Practitioners Act legislated in 1906, see Kazuyuki Nakayasu and Chiaki Sato (n 4) 3.

[7] See Anca M. Cotet and Daniel K. Benjamin (n 4) 407.

[8] Ryan Height Act of 2008, 21 USC § 829 (e) (2) (A) (i); Department of Justice, Drug Enforcement Administration; Implementation of the Ryan Haight Online Pharmacy Consumer Protection Act of 2008; Final Rule. 74 Fed Reg 15,597-15,599 (6 April, 2009)

[9] S. Rep. No. 110–521, pt. 1 at 1-3, 7 (2008).

[10] Ryan Height Act of 2008, 21 U.S.C. § 829 (54).

[11] See Center for Connected Health Policy, State Telehealth Laws & Reimbursement Policies, (Spring 2019) <https://www.cchpca.org/sites/default/files/2019-05/cchp_report_MASTER_spring_2019_FINAL.pdf> accessed 12 June 2019.

[12] See Center for Connected Health Policy, State Telehealth Laws & Reimbursement Policies,(Fall 2018) <https://www.cchpca.org/sites/default/files/2018-10/CCHP_50_State_Report_Fall_2018.pdf>, accessed 12 June 2019, 11.

[13] See for example Kan Stat Ann §40-2, 212 (b) (2018); DC Mun Regs Tit 17, § 4618.4.

[14] See for example ME Regulation § 02-373-6, <https://www.maine.gov/md/laws-statutes/docs/Chapter_6_Telemedicine%20.pdf>, accessed June 12 2019.

munication for the establishment of the relationship or when conducting an examination[15] or prohibiting the use of online questionnaires or telephones for these purposes.[16]

The latest changes to the federal telemedicine regulation in the US have been motivated by the drive to address the opioid crisis.[17] Paradoxically, the limitations of the Ryan Haight Act of 2008 on telemedicine prescriptions[18] have been found to hinder the effective treatment of opioid addiction. As a consequence, the SUPPORT for Patients and Communities Act of 2018 widens opportunities to give telemedicine prescriptions of controlled substances for the purposes of medically assisted treatment of opioid use disorders.[19]

Besides state and federal legislative efforts to use telemedicine to intervene in the opioid crisis, another legislative trend is evident in the US. In recent years, several US states have explicitly required in-person performance of medical abortions.[20] The norms are not justifiable on the basis of the evidence on patient safety[21]; instead, they appear to reflect a political agenda to narrow the rights to abortion in the US.[22] By virtue of the U.S. Supreme Court's ruling in the case of Roe v. Wade, the right to choose an abortion is protected in the US under the right to privacy.[23] More recently, several states have passed extremely strict anti-abortion bills, which would take effect if Roe v Wade were overturned.[24]

[15] See for example 24 Del Admin Code § 1700-19.1, § 1700-19.1,19.3 (2018).

[16] See for example Kentucky Ky Rev Stat § 311.597 3(e) (2015).

[17] Substance Use–Disorder Prevention that Promotes Opioid Recovery and Treatment for Patients and Communities Act P L No 115-271, Preamble, Sec 1 (2018) (SUPPORT for Patients and Communities Act)

[18] Ryan Height Act of 2008, USC § 829 (e)(2)(A)(i), § 802 (54) (2008). In particular, flexibility of the Attorney General to regulate the provision of special registrations for telemedicine-based prescriptions of controlled substances, Ryan Height Act of 2008, § 802 (54)(E)(2008), was never put to practice. Congressional Research Service, The SUPPORT for Patients and Communities Act (PL 115-271): Food and Drug Administration and Controlled Substance Provisions. (15 November 2018) <https://www.everycrsreport.com/reports/R45405.html>, accessed 11 June 2019, 17.

[19] SUPPORT for Patients and Communities Act, P L No 115-271, § 3201-3204, § 3232 (2018); Congressional Research Service, SUPPORT for Patients and Communities Act (n 17), 12-14, 17.

[20] See for example Ind Code § 25-1-9.5-8 (2017) Iowa Admin. Code r 653-13.10 (3) (2013), which was found unconstitutional in Planned Parenthood of the Heartland v Iowa Board of Medicine No 14-1415 (Iowa Sup Ct 2015)

[21] There is no significant difference in the safety of a medical, telemedicine-observed abortion in comparison to the delivery of a medical abortion in person. See Daniel Grossman; Kate Grinday, 'Safety of Medical Abortion Provided Through Telemedicine Compared with In Person' (2017) 130 Obstetrics & Gynecology, 778. However, a quarter of the patients who had been treated with a telemedicine-assisted medical abortion have reported having preferred being treated in person. Daniel Grossman et al. 'Effectiveness and Acceptability of Medical Abortion Provided Through Telemedicine', (2011), 118 Obstetrics & Gynecology, 296.

[22] Rachel Z. Arndt: 'Telemedicine regulations tighten restrictions on medical abortion' Modern Healthcare <https://www.modernhealthcare.com/article/20181219/NEWS/181219888/telemedicine-regulations-tighten-restrictions-on-medication-abortion>, accessed 12 June 2019.

[23] Roe v Wade, 410 US 113 (1973).

[24] 'Louisiana becomes latest US state to pass six-week abortion ban', (The Guardian, 30 May 2010,) <https://www.theguardian.com/us-news/2019/may/29/louisiana-abortion-ban-passes-house>, accessed 12 June 2019; Julian Shen-Berro: 'Trigger Laws' In 7 States Would Ban Abortion Immediately If Roe v Wade Is Overturned',(Huffpost, 23, 2019), <https://www.huffpost.com/entry/trigger-laws-abortion-roe-v-wade_n_5ce5af39e4b0547bd131c788>, accessed 12 June 2019.

In the US, the majority of federal and state norms appear to be justifiable and proportionate on the grounds of maintaining patient safety, a standard of care and preventing abuse of prescription medicine. However, the discrepancies between state rules burdens physicians that offer telemedicine services in multiple states by introducing legal uncertainty. Despite the trends towards more evidence-based telemedicine regulations, such laws are not free from the influence of other political agendas, such as the anti-abortion movement.[25]

PROHIBITIONS ON LONG-DISTANCE TREATMENT IN GERMANY

In Germany, before 2018, remote treatment of patients without any prior face to face examination by a physician was banned by the federal medical chambers.[26] Historically, the ban can be traced back to the nineteenth century. Starting in the 1850s, so-called family magazines targeting an emerging educated middle class featured entertaining articles about the latest scientific discoveries and lifestyle tips.[27] Medical essays were popular and physicians also answered reader's medical questions in the magazines.[28] Furthermore, it was common to advertise medical advice by letter correspondence and physicians even specialised in giving remote treatment only.[29] Many physicians were opposed to this practice, and at the eighth German Medical Assembly on 30 and 31 July 1880 in Eisenach, they voted in favour of a declaration stating that giving medical advice in magazines or in letters was harmful for the reputation of the medical profession and inappropriate.[30] However, the German Medical Assembly, which is a predecessor of today's national medical chamber, had no legislative power. It was merely a meeting of local medical associations.[31] Nevertheless, future professional codes of local medical associations took the declaration into account.[32] In 1896, a draft of a professional code for physicians in

[25] See Planned Parenthood of the Heartland v Iowa Board of Medicine No 14-1415 (Iowa Sup Ct 2015).

[26] § 7 (4) Musterberufsordnung für Ärzte before May 10, 2018, for a comparison of the old and new norm see: <https://www.bundesaerztekammer.de/fileadmin/user_upload/downloads/pdf-Ordner/MBO/Synopse_MBO-AE_zu_AEnderungen____7_Abs._4.pdf> accessed June 3, 2019. The ban however, not prohibit telemonitoring of a patient the physician had examined before. Heike E. Krüger-Brand, 'Telemedizin: Hinweise zur Fernbehandlung' (2016) 113(1-2) Deutsches Ärzteblatt, A8, <https://www.aerzteblatt.de/archiv/173501>, accessed June 3, 2019.

[27] Gunter Mann, 'Medizinische Beratung in Familienzeitschriften des 19. Jahrhunderts und der Ärztestand' (1954) 38 Sudhoffs Archiv 329.

[28] ibid. Interestingly enough, the publishers were aware of the risks of giving medical advice to a patient they hadn't examined before and often included a disclaimer stating that only a physician examining the patient can diagnose an illness; Gunter Mann, 'Die Familienzeitschrift "Ueber Land und Meer" und die Medizin des 19. Jahrhunderts' (doctoral thesis, Goethe-Universität Frankfurt a.M. 1952) 43.

[29] ibid 330; Wolfgang Gerhard Locher, 'Fernbehandlung Gestern und Heute' [2017] Bayerisches Ärzteblatt 514.

[30] 'Der achte deutsche Aerztetag zu Eisenach am 30. und 31. Juli 1880' (1880) 6 Deutsche Medizinische Wochenschrift 452.

[31] ibid 438.

[32] Wolfgang Gerhard Locher (n 29) 515.

the Kingdom of Saxony forbade physicians from treating patients via letter correspondence only.[33]

Later, in 1927, a ban on remote treatment was introduced in the Weimar Republic. The law on sexually transmitted diseases (STDs) stated that it was unlawful for a physician to treat STDs such as syphilis and gonorrhoea via a long distance treatment or to give advice on self-treatment of STDs in writing, illustrations or presentations.[34] Physicians could be criminally liable, with a sentence of up to one year in prison for even offering such health services.[35] Apart from this aspect, the law represented a socially rather progressive and evidence-based approach to the control of STDs, which had been spreading at ever increasing rates since the beginning of the twentieth century.[36] In the discussions regarding the act in the German Reichstag, a member of parliament explained the prohibition saying that physicians should not be allowed to take advantage of inexperienced and uninformed young people.[37]

Until just one year ago, the ban on remote treatment remained in place in professional codes within state legislation. However, with the digitalisation of the healthcare sector, a debate has been going on about its legitimacy, even though the national medical chamber has clarified that even with the ban, telemonitoring would be allowed as long as there is prior face-to-face-examination.[38] An initiative to lift the German ban on long-distance treatment took place on 10 May 2018, when the national medical chamber proposed a change in the federal codes of conduct permitting telemedicine if it is justifiable from a medical perspective and the required due diligence is maintained in the individual case; this emphasises the chamber's view that face-to-face examination should remain the gold standard of medical advice.[39] However, the decision by the national chamber is not binding, because only the federal states' medical chambers have the legislative power to establish professional codes; the national chamber merely issues proposals to encourage uniformed standards.[40]

[33] § 5 Entwurf einer Ständeordnung für das Königreich Sachsen; see Karl Johannes Grosse, 'Die Bestimmungen über die ärztlichen Bezirksvereine im Königreich Sachsen' (1896) 43; available here: https://digital.slub-dresden.de/werkansicht/dlf/93394/45/0/ (accessed June 3, 2019).

[34] § 7 Gesetz zur Bekämpfung von Geschlechtskrankheiten, 18 February 1927, R.G.Bl. 1927, 1 S. 61<http://www.zaoerv.de/01_1929/1_1929_2_b_536_2_541.pdf> accessed June 11, 2019.

[35] ibid.

[36] Albrecht Scholz, Geschichte der Dermatologie in Deutschland (Springer 1999) 282. The law stated an obligation to seek medical care, § 2, but also ensured distribution of preservatives, § 13, and prohibited the quartering of prostitutes, § 17, and therefore fostered women's rights rather than moralisation, see also ibid.

[37] Reichstagsprotokolle 1924/28,8 Sitzung vom 21. Januar 1927, 8691 <https://www.reichstagsprotokolle.de/Blatt2_w3_bsb00000075_00817.html> accessed June 3, 2019.

[38] See Heike E. Krüger-Brand, 'Telemedizin: Hinweise zur Fernbehandlung' (2016) 113(1-2) Deutsches Ärzteblatt, A8 <https://www.aerzteblatt.de/archiv/173501> accessed June 3, 2019.

39 § 7 (4) Musterberufsordnung für Ärzte.

40 § 2 Satzung der Bundesärztekammer.

Of the 16 federal states, 13 have already adopted the proposed phrasing by the national chamber.[41] In the federal state of Baden-Württemberg, the medical chamber amended the norm on the prohibition in a stricter manner than the national chamber, allowing long distance treatment only in pilot projects approved by the chamber.[42] The ban on remote treatment is still in force in Brandenburg and Mecklenburg-Vorpommern, after both medical chambers voted against adopting the national chamber's proposal.[43] Paradoxically, Brandenburg and Mecklenburg-Vorpommern have the lowest population densities in Germany and suffer from physician shortages, which could potentially be solved by telemedicine.[44] On the basis of the freedom to provide services[45], every physician licensed within the EU can offer telemedical services in Brandenburg and Mecklenburg-Vorpommern. Therefore, the state prohibition on remote treatment has the effect of promoting telemedicine services provided by physicians not living there. Hence, patients living in Brandenburg or Mecklenburg-Vorpommern cannot consult via telemedicine with their family physician and would be forced to consult an out-of-state physician if they wish to avail of such services. Furthermore, physicians are discouraged from opening a general practice in these states, since they cannot offer telemedicine as another billable service.

The history of the prohibition on long distance treatments in Germany shows that there is nothing new about contemporary concerns regarding the diminished quality of remotely provided, technology-based medical treatments or regarding their implications for both patient health and the perception of the medical profession. However, modern technologies, such as video connections, provide physicians with much more comprehensive information on the patient's health than the postal system of the 1880s, and should not be subject to similarly stringent prohibitions. Yet, limiting norms are of relevance where technology may enable an abuse of the healthcare system or of pharmaceuticals.

Like the US legal system, the German legal system, with different levels of legislative powers, means there can be different standards for telemedicine at state level. While the recent relaxation of the ban on long-distance treatment addresses the opportunities of modern communication technologies, it has resulted in different norms being applicable

[41] Bayern, Berlin, Bremen, Hamburg, Hessen, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Saarland, Sachsen, Sachsen-Anhalt, Schleswig-Holstein, Thüringen; see their respective Berufsordnung.

[42] § 7 (4) Berufsordnung für Ärzte in Baden-Württemberg; one pilot project of this kind is the telemedicine app Docdirekt by the association of statutory health insurance physicians in the federal state of Baden-Württemberg (KVBW).

[43] § 7 (4) of the respective Berufsordnung; see also <https://www.laekb.de/www/website/design/story/detail.htm?recordid=165CD093F99>;<https://www.aerzteblatt.de/nachrichten/98701/In-Mecklenburg-Vorpommern-vorerst-keine-ausschliessliche-Fernbehandlung> accessed June 3, 2019.

[44] Statistisches Bundesamt, 'Daten aus dem Gemeindeverzeichnis - Bundesländer mit Hauptstädten nach Fläche, Bevölkerung und Bevölkerungsdichte' (2017); see also Radio Berlin Brandenburg, 'Brandenburg hat bundesweit die niedrigste Ärztedichte' (2019) <https://www.rbb24.de/panorama/beitrag/2019/05/aerztemangel-brandenburg-krankenhaus-bundesarztregister.html> accessed June 3, 2019.

[45] See Art 28, Art 56 TFEU.

across German federal states.[46] This regional legal uncertainty may hinder the adoption of telemedicine services within Germany.

CONCLUSIONS

The prohibitions and limitations on long-distance treatments are one of the most straightforward obstacles to the adoption of telemedicine. However, these norms are necessary to ensure patient safety, address public health concerns and preclude abusive practices related to medical care and pharmaceuticals, both on behalf of medical professionals and patients. The norms should be tailored to reflect advances in information technology to deliver healthcare. There will always be contexts where it is paramount to examine and treat a patient in person – for example, when undertaking a neurological examination. However, there is no justification for maintaining prohibitions that were originally targeting the use of non-digital technology, such as post, to communicate with the patients or for allowing norms on the delivery of telemedicine to be influenced by professional lobby groups or political agendas that compromise access to safe medical care. Instead, regulations on telemedicine should be evidence based and reflect the need for safe, high-standard healthcare and other public health interests. Furthermore, especially in federal states, rules and policies should strive to create regional legal certainty. For example, norms that refer to the current standards of healthcare or establish conditions for the quality of technology used for telemedicine may offer the flexibility needed to address the relevance of telemedicine in diverse healthcare contexts and promote further advances in technology.

[46] This unfavourable situation is well illustrated by a service to get a sick note via Whatsapp. AU-schein.de, the company providing the service, is based in Hamburg, whereas the doctors signing the sick notes were based in Schleswig-Holstein or Bavaria because their medical chambers had already lifted the ban on remote treatment, but Hamburg had not at the time the service entered the market. See Armin Himmerath, 'Wie ich mich selbst als arbeitsunfähig einstufte' Spiegel Online (Berlin, April 1, 2019) <https://www.spiegel.de/karriere/krankmeldung-per-whatsapp-wie-ich-mich-selbst-als-arbeitsunfaehig-einstufte-a-1260409.html> accessed June 11, 2019.

BIBLIOGRAPHY

Arndt R, 'Telemedicine regulations tighten restrictions on medical abortion' Modern Healthcare <https://www.modernhealthcare.com/article/20181219/NEWS/181219888/telemedicine-regulations-tighten-restrictions-on-medication-abortion>, accessed 12 June 2019.

Center for Connected Health Policy, *State Telehealth Laws & Reimbursement Policies,*(-Fall 2018) <https://www.cchpca.org/sites/default/files/2018-10/CCHP_50_State_Report_Fall_2018.pdf>, accessed 12 June 2019, 11.

Center for Connected Health Policy, *State Telehealth Laws & Reimbursement Policies,* (Spring 2019). <https://www.cchpca.org/sites/default/files/2019-05/cchp_report_MASTER_spring_2019_FINAL.pdf> accessed 12 June 2019.

Cotet A and Benjamin D, 'Medical Regulation and Health Outcomes: The Effect of the Physician Examination Requirement' (2013) 22 Health Economics 393.

Der achte deutsche Aerztetag zu Eisenach am 30. und 31. Juli 1880, (1880) 6(33) Deutsche Medizinische Wochenschrift 438, 452

Grosse K, 'Die Bestimmungen über die ärztlichen Bezirksvereine im Königreich Sachsen' (1896) 43; available here: <https://digital.slub-dresden.de/werkansicht/dlf/93394/45/0/> accessed 3 June 2019.

Grossman D; Grinday, K, 'Safety of Medical Abortion Provided Through Telemedicine Compared with In Person' (2017) 130 Obstetrics & Gynecology, 778.

Grossmann D; Grindlay, K;Buchacker T Lane, K; Blanchard: 'Effectiveness and Acceptability of Medical Abortion Provided Through Telemedicine', (2011), 118 Obstetrics & Gynecology, 296.

Himmerath A, 'Wie ich mich selbst als arbeitsunfähig einstufte' *Spiegel Online* (Berlin, 1 April 2019); <https://www.spiegel.de/karriere/krankmeldung-per-whatsapp-wie-ich-mich-selbst-als-arbeitsunfaehig-einstufte-a-1260409.html> accessed 11 June 2019.

Krüger-Brand H, 'Telemedizin: Hinweise zur Fernbehandlung' (2016) 113(1-2) Deutsches Ärzteblatt, A8, <https://www.aerzteblatt.de/archiv/173501> accessed 3 June 2019.

Locher W, ‘Fernbehandlung Gestern und Heute’, [2017] Bayerisches Ärzteblatt 514.

‘Louisiana becomes latest US state to pass six-week abortion ban’, (The Guardian, 30 May 2010,) <https://www.theguardian.com/us-news/2019/may/29/louisiana-abortion-ban-passes-house>, accessed 12 June 2019.

Mann G, ‘Die Familienzeitschrift “Ueber Land und Meer” und die Medizin des 19. Jahrhunderts’ (doctoral thesis, Goethe-Universität Frankfurt a.M. 1952) 43.

‘Medizinische Beratung in Familienzeitschriften des 19. Jahrhunderts und der Ärztestand’ (1954) 38 Sudhoffs Archiv 329.

Nakayasu K and Sato C, ‘Liability for Telemedicine’ (2012) 3(1) International Journal of E-Health and Medical Communications 1.

Radio Berlin Brandenburg, ‘Brandenburg hat bundesweit die niedrigste Ärztedichte’ (2019) <https://www.rbb24.de/panorama/beitrag/2019/05/aerztemangel-brandenburg-krankenhaus-bundesarztregister.html> accessed 3 June 2019.

Scholz A, *Geschichte der Dermatologie in Deutschland* (Springer 1999) 282.

Shen-Berro, J: ‘Trigger Laws’ In 7 States Would Ban Abortion Immediately If Roe v. Wade Is Overturned’,(Huffpost, 23, 2019), <https://www.huffpost.com/entry/trigger-laws-abortion-roe-v-wade_n_5ce5af39e4b0547bd131c788>, accessed 12 June 2019.

Statistisches Bundesamt, ‘Daten aus dem Gemeindeverzeichnis - Bundesländer mit Hauptstädten nach Fläche, Bevölkerung und Bevölkerungsdichte’, (2017).

WHO, *Telemedicine. Opportunities and developments in Member States* (Report on the second global survey on eHealth, 2010) 9.

Zhuravlev M, ‘eHealth Regulatory Challenges in Russia’ in this publication.

Teledoctors without borders: The need for a new regulation of telemedicine in Brazil

MARIANA CANTO

From cyberattacks to the public health system database to a controversial telemedicine regulation, telehealth faces new challenges in Brazil.

Keywords: data protection, eHealth, innovation, regulation, telehealth

INTRODUCTION

According to a report published by CB Insights last year[1], from 2012 to June 2018, Apple, Alphabet, Microsoft, Amazon, Facebook, General Electric, Oracle, Intel, Cisco Systems and IBM participated in 209 financing agreements to healthcare and invested a total of $4.7 billion in 25 acquisitions in the industry. These companies invest heavily in research and development as well as in the acquisition of start-ups focusing on health insurance, electronic medical records, telehealth and biotechnology. Currently, Amazon is the technology company with the greatest impact in terms of disruptive technology for the health sector, while Apple is the one with the most functional health records, particularly since the launch of the Apple Watch in 2015.

In Brazil, after the publication of Resolution No. 2.227/2018[2], which aimed to regulate the practice of telemedicine, the Federal Medical Council (CFM) received a high number of criticisms and requests favouring the repeal of the regulation. Due to the uproar of the Brazilian medical community, the CFM's counsellors decided to revoke the resolution and open a public consultation in order to obtain physicians' opinions on the matter. The platform for the submission of proposals was created in mid-February and was originally willing to receive proposals by 7 April. The deadline was subsequently extended to 31 July. This deadline extension aimed to increase the number of suggestions, which totaled more than 1,400 at the time of writing. The outputs will be analysed by a commission created especially to study the suggestions and to present a new proposal to update CFM Resolution No. 1643/2002, which currently regulates telemedicine in the country. In light of this scenario, this article will briefly reflect on the future of telehealth in relation to the social and economic implications of the model in Brazil.

[1] CB Insights, 'Where Big Tech Is Placing Bets In Healthcare' CBInsights (13 September, 2018) <https://www.cbinsights.com/research/top-tech-companies-healthcare-investments-acquisitions/>

[2] Conselho Federal De Medicina. Resolução CFM No 2.227/2018. Brasília: DF. 2018

DOI: 10.5281/zenodo.3297401

THE BRAZILIAN PANORAMA

For developing countries with difficult-to-access regions, as is the case in Brazil, telehealth can be especially important. Overcoming physical and geographical barriers by using technology in health practices makes this tool valuable and indispensable in many cases. Several Brazilian initiatives illustrate the development of telehealth in the country. The most important examples include the National Telehealth Program, the National Network of Teaching and Research (RNP) and the Telemedicine University Network (RUTE).

Telemedicine services differ from state to state in terms of their evolution and type. The state of Minas Gerais, for example, has focused on implementing an electrocardiogram (ECG) service at a distance due to the importance of cardiovascular diseases in the state's epidemiological profile. In Rio Grande do Sul, the first service in Brazil for telediagnosis for chronic respiratory diseases was implemented due to a high prevalence of cases. Despite the development of telemedicine in several states in the south and southeast of Brazil, the unequal regional distribution of the practice is especially clear when we look at the range of services offered in the north and northeast regions, which are the regions most in need of services and where access to healthcare services by those who live far from urban centres is practically non-existent.

However, even though the development of telemedicine in those regions is possible, the lack of definition in the new regulation regarding what can be considered a "geographically remote area" was another point of concern raised by doctors. The reason for this concern was that this could encourage the unrestrained use of teleconsultation and increase the distance of the doctor-patient relationship. The new law would allow patients in more remote regions of the country to have first medical consultation provided at a distance as long as this was guided by another health professional who is not a doctor, such as a nursing assistant. In this way, according to the new resolution, the requirements for a consultation for those who lived in difficult-to-access places would be fewer than for those who lived in city centres, as the latter could not opt for remote consultations during first time visits. Also, in case of consecutive consultations, the city residents who opt for teleconsultations, would have to always alternate face-to-face consultations with the remote ones.

The resolution is emerging at a time when remote cities are faced with support deficits. The situation has worsened since the departure of Cuban professionals from the *Mais Médicos* programme, who decided to leave the country after heavy criticisms were made by the president Jair Bolsonaro. The indigenous people, isolated and distant from the great city centres, are the most affected population; of the 372 professionals that served this population, 301 were Cubans.[3] In a large country such as Brazil, the use of ICT systems can help to reduce cultural, socio-economic and geographic barriers to accessing health services

[3] Thais Lazzeri, 'Transplantada ou cardiopata? Falta de dinheiro faz médicos escolherem qual criança indígena atender' The Intercept Brasil (10 April 2019) <https://theintercept.com/2019/04/09/saude-indigena-ongs/>

and information, reducing the need to go to the centres in certain cases. However, as the practices of telehealth have grown throughout the country, discussions regarding ethical and legal criteria have also arisen.

RESOLUTION NO. 2.227/2018 AND THE BACKLASH TO IT

Privacy, professional practice, interoperability of information systems and the effectiveness and safety of the equipment used are the key points of the laws that regulate the practise of medicine in Brazil. On 3 February 2019, the Federal Council of Medicine (CFM), substituted Resolution No 1.643/ 2002[4], which regulates the practice of telemedicine in Brazil, with Resolution No. 2.227/ 2018, which allows consultations, diagnoses and even surgeries from a distance, both in the public system, the SUS (Brazilian Unified Health System), and in the private health system. However, a few weeks after its publication, on 22 February, the CFM decided to revoke the resolution after a great backlash from the Brazilian medical community.

In Brazil, the medical profession's regulatory instrument is the Code of Medical Ethics (CEM). Its Article 37 is highly relevant for telemedicine, since it prohibits the prescription of treatment or other procedures without directly examining the patient, except in urgent or emergency cases or where it would otherwise be impossible. In the same direction, CFM Resolution No. 1.643/ 2002 – the current telemedicine regulatory instrument – restricts the use of telemedicine by defining it as the practice of medicine through the use of interactive communication, audiovisual technologies and data methodologies for assistance, education and research purposes in health. Thus, until the new text is approved, telemedicine will be subject to the terms of CFM Resolution No. 1643/2002, which does not allow teleconsultation, telesurgery, telemonitoring or teleconferencing for a surgical act.

In addition to the lack of debate about the regulation, one of the most important issues raised in the comments and criticisms made of the 2018 Resolution was in relation to patients' privacy, as the resolution required a considerable amount of data from virtual medical appointments. However, the resolution does not make it clear how the data would be stored in order to avoid leaks or breaches of sensitive data or confidentiality. Considering the recent approval of the Brazilian General Data Protection Law (LGPD), the lack of clarity regarding the collection and treatment of patients' data and other specific legal risks when using virtual care are crucial issues raised by the medical and legal community. As mentioned, this resolution is essential to regulate issues that still need to be clarified, especially in terms of data protection, AI-specific regulation and accountability for possible medical errors.

[4] Conselho Federal De Medicina. Resolução CFM No 1.643/ 2002. Brasília: DF. 2002

After the CFM repealed the resolution, the Association of Medicine of São Paulo (APM) released research on the subject, conducted in partnership with the *Global Summit Telemedicine & Digital Health*.[5] The survey of March 2019 presented a comprehensive overview of the topic from the perspective of the doctors of São Paulo. In the results, 80% of physicians said they use these technologies in patient care and 90% said that they use the technologies in hospitals and clinics where they work. According to the research, 80% of the interviewed doctors are favourable to using *WhatsApp* and other social networks when treating patients. The study also shows that 98% of physicians agree with the regulation of telemedicine, which covers issues ranging from distance care to medical reports. Regarding teleconsultations and teleprescriptions, opinions were divided. 50% favour electronic prescriptions after face-to-face consultation while 49% do not agree. On the other hand, 45% agreed with distance consultations after one face-to-face meeting, and 55% were against them, even if the first consultation was in person.

Regarding the revocation of the resolution, 76% stated that they were dissatisfied because they were not consulted about the change. Another noteworthy finding in the survey is the number of professionals in favour of making available patients' health information in a digital cloud (85%), as long as data protection standards are met. Of the amount, 94% believe that sharing information can help the professionals, patients and system.

CYBERATTACKS AND THE LACK OF BEST PRACTICES

It is necessary to remember that vulnerable populations are or will become patients of telehealth services not only in Brazil but in many other countries. Privacy policies and terms of the confidentiality of the physician-patient relationship must be easily accessible to users as extremely sensitive data is often collected and stored. Data protection laws and specific laws and resolutions are the primary actors in such cases, as they are necessary in order to establish and regulate the details of the collection, storage and treatment of medical data.

Information and communication technology systems that support the various types of telemedicine and telehealth activities and practices can give rise to various vulnerabilities to threats and risks to patients' data security, privacy and confidentiality. Several studies[6] show that, in Brazil, developers and users of telehealth systems have little concern for adopting good practices and seeking national and international certifications, such as SBIS,

[5] Associação Paulista de Medicina. Pesquisa 'Tecnologia e Saúde'. March 2019 <http://www.apm.org.br/newsletter/comunicacao/2019/arquivos/02_Pesquisa_APM_GS_04.04.2019.pdf>

[6] Sabbatini, R 2018, 'Normas e boas práticas de segurança, privacidade e confidencialidade de plataformas de teleassistência em saúde', in (D. Garrido; P. Dias; A.E. Oliveira; H.O. Serra), Anais do 8º Congresso Brasileiro de Telemedicina e Telessaúde, 10.

CFM, CFO, ISO and others[7], especially for registration systems, i.e. databases and software that store and manipulate identified information. Recently, this point was proven during a cyberattack on the Unified Health System (SUS) database. The leak of personal information such as full names, addresses, social security numbers and birth dates of 2.4 million system users was exposed on 11 April 2019.

According to the media[8], the failure was in the SUS integration system with other applications, in a part of its API. The API used in the SUS registration system, *Cadsus*, had a function to query data after users logged in and entered their password in the system. In order to achieve that, a URL was generated. For example, in the address "consulta.php?-dados=http://xxx.xxx.xxx.xx", the Xs at the end of the address are the 11 social security (CPF) numbers of the user who made the query. The API associated the users' CPF with their data, and returned with the complete data about them. The attacker understood that this was a loophole and tested an algorithm capable of testing 300 million valid combinations, obtaining the users' personal data from the CPF of each one of them. Although it is believed that only 1% of system users were exposed, this type of attack can be performed relatively easily by someone with some technical knowledge or by someone with some technical knowledge or easily identified in a system audit at an earlier moment, which proves the seriousness of the problem.

CONCLUSION

Telehealth offers the potential to solve major contemporary health challenges, and Brazil has the right characteristics for its full use. The country has continental dimensions, a population of 200 million and a public unified health system. In addition to its size, the existence of thousands of isolated and difficult-to-access places with a scarcity of health services and extremely unequal distribution of medical resources indicate the great potential of telemedicine expansion in the country.

From the Brazilian social perspective, telemedicine has the potential to promote a greater integration of the health system, adding efficiency and reducing costs. It can overcome the geographical barriers that act as an impediment to realising the fundamental right to health services. Regarding the economic situation of the country, telemedicine is a source of innovation and incorporates technological advances from other areas, such as information and communication technologies, microelectronics, computing and telecommunications. Due to its interdisciplinary nature and its dynamic interrelations, it has the potential to boost different industries in the country.

[7] Plinio Sá Leitão-Junior et. al, 'Safety regulation of health electronic information: an overview' (2016) 1(8/4) J. Health Inform. 2016 8(4):148-55 <http://www.jhi-sbis.saude.ws/ojs-jhi/index.php/jhi-sbis/article/viewFile/415/278> accessed 27 March 2019

[8] Márcio Padrão, 'Dados pessoais de 2,4 milhões de usuários do SUS são vazados na internet' UOL (São Paulo, 11 April 2019) <https://noticias.uol.com.br/tecnologia/noticias/redacao/2019/04/11/dados-pessoais-de-24-milhoes-de-usuarios-do-sus-sao-vazados-na-internet.htm>

Despite the importance of technological advances, the originally proposed text of the new resolution was problematic in several respects. It made physicians and patients vulnerable, since it stipulated that the teleconsultation would be recorded,. The lack of good practices, leading to medical data breaches, shows the security flaws in Brazilian systems. Also, the country is still struggling to implement its newly approved General Data Protection Law (LGPD), and to raise awareness of the level of security necessary for the collection, storage and treatment of sensitive data. The protection of patient's health data in Brazil still represents a major barrier to a greater and safer adoption of telemedicine in the country.

Another aspect that should be reviewed after the public consultation is the lack of transparency regarding the range of medical procedures permitted, which raised concerns about the possibility of commercialising medicine. As Dr. Chao Lung Wen, associate professor and head of the telemedicine discipline at the University of São Paulo believes, true telemedicine must be responsible, efficient and sustainable, with ethical and legal grounds, norms and digital security, accreditation of services and periodic monitoring, with regulations that can stop its exploitation and commercialisation.

Finally, there is still a need to articulate the idea of equity and to be careful with policies that tend to homogenise. The search for a pattern of distribution of goods and services should not override the necessity to address the needs of minority groups, such as vulnerable populations. Only in this way will it be possible for the whole country to see and benefit from the improvements brought by telehealth.

BIBLIOGRAPHY

Associação Paulista de Medicina. Pesquisa "Tecnologia e Saúde". March 2019 <http://www.apm.org.br/newsletter/comunicacao/2019/arquivos/02_Pesquisa_APM_GS_04.04.2019.pdf >

CB Insights, 'Where Big Tech Is Placing Bets In Healthcare' CBInsights (13 September, 2018) <https://www.cbinsights.com/research/top-tech-companies-healthcare-investments-acquisitions/>

CONSELHO FEDERAL DE MEDICINA. Resolução CFM No 1.643/ 2002. Brasília: DF. 2002

CONSELHO FEDERAL DE MEDICINA. Resolução CFM No 2.227/2018. Brasília: DF. 2018

JMSV Maldonado et al. 'Telemedicine: challenges to dissemination in Brazil' Cad. Saúde Pública, Rio de Janeiro, 2016 <http://www.scielo.br/pdf/csp/v32s2/pt_1678-4464-csp-32-s2-e00155615.pdf> accessed 15 April 2019

Márcio Padrão, 'Dados pessoais de 2,4 milhões de usuários do SUS são vazados na internet' UOL (São Paulo, 11, April 2019) <https://noticias.uol.com.br/tecnologia/noticias/redacao/2019/04/11/dados-pessoais-de-24-milhoes-de-usuarios-do-sus-sao-vazados-na-internet.htm>

Plinio Sá Leitão-Junior et. al, 'Safety regulation of health electronic information: an overview' (2016) 1(8/4) J. Health Inform. 2016 8(4):148-55 <http://www.jhi-sbis.saude.ws/ojs-jhi/index.php/jhi-sbis/article/viewFile/415/278> accessed 27 March 2019

Sabbatini, R 2018, 'Normas e boas práticas de segurança, privacidade e confidencialidade de plataformas de teleassistência em saúde', in (D. Garrido; P. Dias; A.E. Oliveira; H.O. Serra), *Anais do 8º Congresso Brasileiro de Telemedicina e Telessaúde*, 10.

Thais Lazzeri, 'Transplantada ou cardiopata? Falta de dinheiro faz médicos escolherem qual criança indígena atender' The Intercept Brasil (10, April 2019) <https://theintercept.com/2019/04/09/saude-indigena-ongs/>

People will consult a health app rather than a doctor when they‘re sick.

Virtual consultants and e-communications
between doctors and patients will become the norm.

People will be treated with comprehensive assistance from artificial intelligence
and receive 24/7 comprehensive healthcare monitoring.

What will be the most important development in eHealth by 2040?

There’ll be a movefrom wearables to "insideables"
that track the human body from within.

There’ll be a tension between obligatory and voluntary health monitoring.

We’ll have better management of chronic diseases by monitoring them from home.
Appointments will be booked when health deteriorates.

Cyborg Human Parity Act

Deregulation

Robust legal and ethical measures for dealing with automated diagnostic and consultant systems.

Awareness of societal reasons for health and diseases.

What policy measures does the change require?

Strict rules on accessing health data.

Regulations on vsales of private health data to third parties, to ensure trust in eHealth systems.

Interoperability

Cybersecurity

AUTHORS

Dr **Btihaj Ajana** is senior lecturer at the Department of Digital Humanities, King's College London. Her academic work is interdisciplinary in nature, spanning areas of digital culture, media praxis and biopolitics. She is the author of Governing through Biometrics: The Biopolitics of Identity (Palgrave, 2013) and editor of Self-Tracking: Empirical and Philosophical Investigations (Palgrave, 2018) and Metric Culture: Ontologies of self-tracking practices (Emerald, 2018).

Prof. **Nachmam Ash** has been a military physician for 25 years. He retired in the rank of brigadier general as the surgeon general of the IDF. For the last 5 years, he has been the chief medical officer of MHS. Ash is a faculty member in the School of Health Sciences, the Department of Health Systems Management in Ariel University. His main academic interests are medical informatics and community healthcare.

Dr. **Paola Aurucci,** University of Turin and Center for Advanced Technology and Wellbeing (San Raffaele Hospital, Milan). Author biography: PhD in comparative law at the State University of Milan. Since 2018, she has been a post-doctoral fellow in law and technology at University of Turin (Italy) and a researcher expert on data protection compliance at the Center for Advanced Technology and Wellbeing (San Raffaele Hospital, Milan).

Dr. **Thomas Christian Bächle** is head of the Digital Society Research Programme at the Alexander von Humboldt Institute for Internet and Society (HIIG) in Berlin. Since April 2019 he has also been guest professor at the Hermann von Helmholtz Centre for Cultural Techniques at the Humboldt University of Berlin. He leads the research project "The Futures of Telemedicine: Knowledge, Policy, Regulation", which focuses on regulatory challenges, norms and the acceptance of practices and applications in the field of eHealth. His areas of research include cultural representations of identities, bodies and (media) technologies; human/machine interaction; technological materialities, interfaces and agency; mobile media, surveillance, robotics, affective computing and simulation technologies.

Stefaan Callens is a professor of health law at KU Leuven and a lawyer at the Brussels bar. He is a member of the Belgian Royal Academy of Medicine.

Mariana Canto is a researcher at the Recife Institute for Research on Law and Technology (IP.rec) and holds a Bachelor of Laws (L.L.B.) from the Federal University of Pernambuco, Brazil, having studied part of her programme at the University of Hamburg, Germany. Mariana also worked with the Secretariat of the Internet Governance Forum (IGF) at the United Nations and was a fellow researcher at the Brazilian National Council for Scientific and Technological Development (CNPq).

Valeska Cappel, Dipl. Soz. studied sociology, political science and European migration at Johannes Gutenberg University in Mainz. She graduated with a thesis on moral nutrition change. From 2015 to mid-2017, she worked in the field of online research in a private-sector consulting firm, where she developed coding concepts for content analysis. For 2017 to 2018, Ms. Cappel received a scholarship from the Graduate School of Humanities and Social Sciences at the University of Lucerne (GSL) and since then she has been working on her doctorate on the digitisation of the health system, the emergence of classifications in preventive health apps and their practical application.

Sandra Diehl is associate professor at the Department for Media and Communication Studies at the Alpen-Adria University of Klagenfurt, Austria. She received her PhD and her habilitation in business administration from Saarland University in Germany. Her research interests include media and convergence management, international and intercultural advertising, CSR and health communication. Sandra Diehl has published in numerous journals, such as the International Journal of Advertising, Advances in International Marketing, Advances in Consumer Research and European Advances in Consumer Research. She has authored and edited several books, among them Advances in Advertising Research. She is also board member of the European Advertising Academy.

Karolin Eva Kappler, PhD, is a researcher at the Chair of Business Information Systems at the University of Hagen. Currently, she coordinates the project “AI as 'virtual citizens' in a plural and dynamic society", funded by the Volkswagen Foundation. Since 2009, she has been carrying out (applied) research on digitalisation, first at the Technology Innovation Research Center Barcelona Media in the fields of information, technology and society, and later as part of the DFG-funded project “Taxonomies of the Self. Emergence and social generalisation of calculative practices in the field of self-inspection” at the Institute of Sociology (University of Hagen). She has published numerous articles in journals and books on the topics of social media, self-tracking, big data, calculative practices, network analysis and violence in everyday life.

PD Dr. **Veronika Karnowski** (PhD, 2008, University of Zurich; Habilitation, 2018, LMU Munich) is currently a visiting professor at the Institute of Communication and Media Studies, Leipzig University. Her research focuses on mobile media, social media and news, as well as eHealth and mHealth.

Anastasiya Kiseleva holds an LL.M. in IP & IT law (EULISP) from Leibniz University Hannover (magna cum laude) and completed a master's thesis on "Authorship and Ownership of Works Generated by AI". Her current research interest is in the area of IP & IT law and health.

Irma Klünker is a student assistant at the Alexander von Humboldt Institute for Internet and Society in the research project "The Futures of Telemedicine". She is a law student at Humboldt University, specialising in intellectual property law in the area of biotech innovations.

Isabell Koinig is a postdoctoral researcher at the Department of Media and Communication Studies at the Alpen-Adria University of Klagenfurt, Austria. She just finished her dissertation investigating how different pharmaceutical advertising appeals were received in a cross-cultural context. Her research interests predominantly concern the fields of health communication, intercultural advertising, organisational developments and communication practices, CSR reporting and media and convergence management.

Prof. **Azi Lev-On** is a faculty member in the School of Communication in Ariel University. His research focuses on the social and political uses and perceived effects of social media, including public participation and deliberation online, online communities, collective action and campaigns, and behaviours in computer-mediated environments, employing a variety of methods such as content analysis, interviews and laboratory experiments.

Galit Madar is a doctoral student in communications and health systems management. Her research focuses on the evolving interactions between family physicians and their patients, as technology mediates between them and reshapes the role of family physicians.

Manisha Mantri, manishar@cdac.in, Centre for Development of Advanced Computing, C-DAC, Pune, India.

Trix Mulder is PhD Candidate at the Security, Technology and e-Privacy research group at the Faculty of Law at the University of Groningen.

R. Rajamenakshi, menakshi@cdac.in, Centre for Development of Advanced Computing, C-DAC, Pune, India.

Daniela Rudner works as a senior technical advisor for the Pretoria office of The Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH. Daniela manages cooperation projects with the private sector, among them Unjani Clinics, in partnership with Imperial Health Sciences.

Arun Shroff is an entrepreneur using AI to address global healthcare challenges at Xtend.AI. He is currently a topic driver for ophthalmology at the ITU/WHO Focus Group on AI for Health.

Dr. **Nao Sipula** is the CEO of WatIF Health, Benoni, South Africa, responsible for the business's strategic direction and global implementation of the ground breaking WATIF Health Portal.

Martin Stojanov is a PhD student in information systems at the Department of Informatics and Media at Uppsala University. His research focuses on datafication in public health, and he has conducted empirical research on self-tracking and public health surveillance.

Dr. **Freya Sukalla** (PhD, 2017, University of Augsburg) is a postdoctoral researcher at the Institute of Communication and Media Studies, Leipzig University. Her research focuses on media processing and effects and health communication.

Gaur Sunder, gaurs@cdac.in, Centre for Development of Advanced Computing, C-DAC, Pune, India.

Lauren Tonti is a doctoral candidate at the Max Planck Institute for Social Law & Social Policy. Before earning her master's degree in public health from the Harvard T.H. Chan School of Public Health in 2018, Lauren received a Juris Doctor from Case Western Reserve School of Law and a Bachelor of Arts degree from Wellesley College. Lauren is also a member of the New York State Bar.

Lynda Toussaint is the CEO of Unjani Clinics NPC, Centurion, South Africa, an enterprise development initiative with the intention to empower black female professional nurses to own and operate primary healthcare container clinics in the rural and township communities of South Africa.

Niklas Trinkhaus is a student assistant at the Alexander von Humboldt Institute for Internet and Society in the research project "The Futures of Telemedicine". He has a special interest in the potentials of digitalisation for public health and the associated challenges. Before Niklas worked as a research assistant at the Institute for Democracy and Civil Society (IDZ) in Jena.

Alina Wernick is a researcher at the Alexander von Humboldt Institute for Internet and Society who contributes to the Futures of Telemedicine and Data Governance projects. As a legal scholar, she is interested in interdisciplinary research on data protection, health, intellectual property and competition law. She has completed the International Max Planck Research School for Innovation and Competition and is finalising her thesis on patent law and open innovation at the Ludwig Maximilian University of Munich.

Verina Wild, Sarah Akgül, Katharina Eisenhut, Tereza Hendl, Bianca Jansky, Felix Machleid, Niels Nijsingh, Nicole Peter and **Ela Sauerborn** are members of the "META" research team (acronym for "mHealth: Ethical, legal and social aspects in the technological age") at Ludwig-Maximilians-University Munich. The research team includes scholars from various disciplines, including philosophy, applied ethics, sociology, legal studies, medicine and public health. The goal of the META project is to thoroughly analyse the ethical, legal and social aspects of mobile health technologies such as apps and wearables. The project investigates the possibilities and challenges of mHealth as well as broader aspects of the digital transformation at the individual, population and global level. It is funded by the German Ministry of Research and Education (BMBF) and runs from 2018–2024. Verina Wild is the principal investigator. She is a bioethicist and deputy director at the Institute of Ethics, History and Theory of Medicine at the Ludwig-Maximilians-University, Munich.

Mikhail Zhuravlev is a junior research fellow at the International Laboratory for Information Technology and Intellectual Property Law and a lecturer at the Department of Information Law of the National Research University Higher School of Economics (Moscow). Mikhail's research interests include data protection law and the legal issues associated with machine learning. In 2016, Mikhail graduated from a master's programme on IT and IP law in Moscow. Currently Mikhail is focusing on his PhD thesis, which examines the legal aspects of information security in telemedicine.

IMPRINT

PUBLICATION
July 2019

EDITORS
Dr. Thomas Christian Bächle (HIIG)
Alina Wernick (HIIG)

Alexander von Humboldt Institute for Internet and Society
Französische Straße 9
10117 Berlin
Germany
www.hiig.de/en

LAYOUT
Katja Margulis (www.lastica.berta.me)
Larissa Wunderlich (HIIG)

Softcover ISBN: 978-3-9820242-3-3
eBook ISBN: 978-3-9820242-4-0

Alexander von Humboldt
INSTITUTE FOR INTERNET
AND SOCIETY

ISBN: 978-3-9820242-3-3