



HARVARD



“MOBILE TECHNOLOGY-BASED SERVICES FOR GLOBAL HEALTH AND WELLNESS: OPPORTUNITIES AND CHALLENGES”

*Summary of Main points from the OECD-HARVARD
Global Health Institute Expert Consultation of 5-6
October 2016.*

This document reports on key issues emerging from the OECD Expert Consultation: “Mobile Technologies Based Services for Global Health and Wellness: Opportunities and Challenges (<http://www.oecd.org/sti/ieconomy/mobile-technology-based-services-for-global-health.htm>)”. The Consultation’s objectives were to further international dialogue on issues critical for the successful adoption of mobile-technology-based services for health and wellness with a special focus on privacy, security, quality assurance challenges and measurement needs for evidence-based policy-making.

The Expert Consultation was held on 5-6 October, 2016 in Boston (US) at The Harvard Global Health Institute, in collaboration with Swedish Vinnova, Canada Health Infoway and the Global Coalition on Aging. Their financial support and that of participating member countries is gratefully acknowledged.

This report was drafted by Elettra Ronchi (Senior Policy Analyst , Digital Economy and Policy Division, OECD), Liana Rosenkrantz Woskie (Assistant Director Harvard Global Health Institute Strategic Initiative on Quality, US ; London School of Informatics, UK) and Julia Adler Milstein (Associate Professor, University of California, San Francisco, US) based on inputs from workshop experts, the OECD Health Committee and the OECD Working Party on Security and Privacy in the Digital Economy. It summarises discussions and presentations and includes post-consultation feedback received on possible next phases of OECD work.

Particular thanks and recognition is extended to Ashish Jha (Director, Harvard Global Health Institute, US), Yves-Alexandre de Montjoye (Assistant Professor, Imperial College Data Science Institute and Department of Computing, UK), Jenni Nordborg (Head of the Bioentrepreneurship Department, Health Division at VINNOVA, Sweden) , Taylor Reynolds (Director, Technology Policy at the Massachusetts Institute of Technology, US), Effy Vayena (Professor, Swiss Federal Institute of Technology in Zurich) , Michael, W. Hodin (Executive Director of the Global Coalition on Ageing, US), Jennifer Zelmer (President of Azimuth Health Group and Adjunct Professor University of Victoria, Canada), for their contribution and directions provided to this project. The authors would also like to acknowledge Christine Azzaro (Program Administrator, Harvard Global Health Institute, US) and Claire Hilton (Junior Research Assistant, OECD) for the support in managing and organising the workshop.

The opinions expressed and the arguments employed herein do not necessarily reflect the official views of OECD countries.

This document, as well as any data and any map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

TABLE OF CONTENTS

INTRODUCTION	4
The OECD-HARVARD Global Health Institute Workshop	5
BACKGROUND	7
Policy Context and Recent Developments.....	7
The Need for Integrated Approaches in Promoting Trust	9
GLOBAL EXPERIENCES WITH MHEALTH AND ASSOCIATED POLICY CHALLENGES	11
Using Mobile Phone Data to Model and Predict the Spread of Infectious Diseases	11
Connected Health Delivery System for Remote Care in Korea.....	12
MHealth Solutions for Improved Maternal and Newborn Care	13
MHealth for Better Adherence to Therapeutic Guidelines and Protocols in Low Resource Settings	14
FRAMEWORKS AND TOOLKITS TO SUPPORT MHEALTH ADOPTION AND SCALING	17
The WHO MHealth Assessment and Planning for Scale Toolkit	17
Identifying Dimensions of Foundational MHealth Policies.....	18
APPROACHES TO THE EVALUATION OF SAFETY, EFFECTIVENESS, AND PRIVACY PROTECTION OF MHEALTH APPs	20
The MHealth App Regulatory Environment	21
RECONCILING RISKS AND BENEFITS OF DATA USE : EXAMPLES OF RECENT POLICY ACTIONS	24
The OECD Recommendation on Health Data Governance	24
Enhancing patient access to and control over their data	25
New Consent Models	25
Right to Data Portability	26
Enhancing individuals' access to their own data.	26
New Health Data Cooperatives	27
PRIORITY AREAS FOR FUTURE COLLABORATIVE EFFORTS	28
Support an Agenda for Evidence-based Implementation of mHealth	28
Support the development of Internationally-agreed Quality Assurance Criteria for Health and Wellness Apps	28
Examine the Opportunities and Challenges in Enhancing Users' Access and Control over their Data	28
REFERENCES	30

INTRODUCTION

Since 2008, the Organisation for Economic Cooperation and Development (OECD) has led an effort to help countries improve the evidence base for policy-making to promote the adoption and use of information and communication technology (ICT) in the health sector as well as support the realization of associated economic and social benefits.

The 2016 OECD-Harvard Global Health Institute workshop on “Mobile Technologies Based Services for Global Health and Wellness: Opportunities and Challenges”¹ built on these efforts and addressed progress in the implementation of mobile health technologies (mHealth) as well as enabling frameworks and challenges. With the growth in Internet connectivity and smart/mobile devices, there is substantial interest across OECD countries in fostering the availability, and effective use, of mHealth to improve health care delivery and ultimately, the health of populations. In parallel, there is recognition that mHealth poses unique challenges that current eHealth policies may not be fully equipped to address.

In particular, over the past few years there has been significant mHealth adoption and use that has been accompanied by research and assessment that begins to address issues of integration of mobile phone technology into healthcare systems at scale. This work has highlighted the ability of mobile phone technology to deliver greater health system efficiencies, to collect high-quality data for disease outbreak tracking, prevent stock-outs of medication, assist in patient adherence to treatment programs (particularly among seniors and difficult to reach populations) and improve access to health care, among other benefits. More broadly, the proliferation of smartphones has created demand for health and wellness mobile applications or “apps” (software programs on mobile devices), which hold particular promise for patient self-monitoring and management of non-communicable diseases (NCDs) such as diabetes and cardiac disease and other health conditions where continuous interaction is imperative. The breadth of mHealth capabilities results in their broad appeal to both high and low income countries. For high income countries, using mHealth to address challenges related to caring for non-communicable diseases and an ageing population are top priority while in low income countries, disease monitoring and other public health priorities drive the mHealth agenda.

Despite such progress and widespread recognition of the potential of mHealth, identifying mHealth solutions that are safe, effective, and trustworthy, and then implementing them at scale pose significant challenges. As such, mHealth is currently at a critical juncture in its evolution. Early efforts saw many trials funded by operators, governments, NGOs and other interested bodies. In 2011, there were an estimated 800 mHealth projects deployed worldwide, of which 119 were in Europe. In 2013, the Boston Consulting Group estimated 500 mHealth programs and in 2015 the number of patients using mHealth apps was estimated at approximately 500 million globally. Reports from the first quarter of 2014 show that there were about 100.000 mHealth apps listed in the two major app stores (Apple and Android). The rapid proliferation of mHealth pilots and the growth of health and wellness apps have emerged as significant challenges for policymakers. Many of the mHealth pilots were not designed to scale and instead intended to demonstrate proof of concept. This has led to issues with fragmentation in financing, short-term partnerships, and lack of integration into formal health systems. Health and wellness apps, unless classified as medical devices, are largely unregulated and although leading players, such as Apple, are taking steps to provide guidance for developers, and self-regulatory standards are emerging, there is a need to better understand the safety and effectiveness of those apps which are not already addressed by specific legislation. In addition, in order to function, health and wellness apps may require a vast trove of personal data, raising privacy and security concerns. Thus, data governance and associated mHealth policies are currently high on the policy agenda of countries deciding how best to leverage mHealth for improved population health.

The OECD-HARVARD Global Health Institute Workshop

In order to learn about ongoing efforts and identify priorities for future actions to support evidence-based mHealth policies, the OECD and Harvard University convened a two-day meeting in October 2016. The meeting sought to highlight country-level insights and provide a platform for shared learning across countries as well as discuss priorities for future collaborative efforts.

Specific topics included:

- Global trends and examples of mHealth applications in OECD and non-OECD countries for prevention, health promotion, diagnosis, access to treatment, treatment adherence, monitoring pharmacovigilance and disease surveillance. These examples served to reveal domains in which new policies may be needed.
- Measurement needs for evidence-based mHealth policymaking and for creating an environment of trust in mHealth solutions.
- Privacy, security and quality assurance challenges raised by “big data” collected through mobile technologies for health care, public health and disease surveillance purposes (e.g. health emergency response to Ebola).
- Documentation of the development of relevant frameworks, recommendations to promote the implementation of robust health-related data governance practices, and perspectives on policy and research priorities.
- High-priority policy needs and possible feasible avenues for progress in measurement that could better inform policies in those priority areas.

The following key themes emerged from the meeting:

- Given the rapidly evolving mHealth landscape, policymakers have few available frameworks and toolkits to guide their actions. Many are wrestling with the same issues and learning in parallel (rather than together). It is therefore important to identify the frameworks and toolkits that need to be more widely disseminated and can serve as tools to facilitate collaborative learning.
- Innovative new measurement toolkits like the World Health Organisation (WHO) mHealth Map are needed to inform resource allocation and the effective implementation of mHealth programs. The mHealth Map toolkit assists mHealth project teams to critically assess their mHealth project as they move from piloting to planning their next steps for overcoming the challenges inherent in scaling up.
- Governance frameworks, such as the recently adopted OECD Recommendation on Health Data Governance, are needed to help create an environment in which personal data can be used in the public interest without compromising individual privacy, autonomy and fairness. The process of implementation and the development of explanatory material should be pursued to assist countries in implementing this Recommendation.
- MHealth smartphone applications (apps) are becoming increasingly prevalent and creating a new generation of safety, effectiveness, and privacy/security challenges that need to be better understood in ways that inform and guide policymaker actions. Health-related app accreditation programs, in which apps are subject to formal assessment or peer review (e.g., app rating systems), as well as guidance on good practice in privacy, security and safety (e.g., the EC 2016 voluntary draft code of conduct on privacy for mHealth apps for app developers), are important developments that aim to provide assurances about

quality and safety, foster trust, and promote app adoption by patients and professionals. There is an opportunity for cross-country collaboration to develop policy strategies that promote such trust. For example, agreement on standards for accreditation processes and coordinated quality assurance processes are needed for enabling the health potential of apps.

- Empowering individuals with the knowledge and skills to manage their own personal health data when using mHealth will help develop greater trust in these services and apps. A number of emerging initiatives aim to enhance consumers' access to and control over their data. Some of these initiatives relate to data held by public bodies but others encourage private enterprises to give consumers access to their data including by setting out a "right to data portability". There is an evidence gap in this area and analytical work to support policy-making is needed.

This report is an effort to summarize the background materials that set the stage for the event, topics presented and discussed during the workshop, and identify opportunities for cross-country collaborative actions to advance evidence-based mHealth policies.

BACKGROUND

Several well-recognized organizations have put forth definitions of mHealth. For example, the World Health Organisation (WHO) defines mHealth as a component of eHealth, a “medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices.”¹

MHealth definitions have also included applications (apps), such as lifestyle and wellbeing apps that may connect to medical devices or sensors (e.g., bracelets or watches), as well as personal guidance systems, such as health information and medication reminders provided by SMS and telemedicine. The former group handles low-confidentiality data (personal wellness and activity data); this is usually a consumer-driven purchase and strong consumer interest has attracted many companies into the space. The second group generally manages medium to high confidentiality data (health data and personal medical records); these are used by clinicians, patients or hospital system reporting. MHealth solutions in the second group are contributing to new opportunities for the integration of mHealth into existing health services in both higher- and lower-income countries and offer significant potential to improve healthcare outcomes.

Alongside definitions, a range of mHealth frameworks exist. One set of frameworks characterizes mHealth according to technologies and processes.² A second set of frameworks focuses on the desired impact of mHealth and applications to achieve specific health outcomes (from both patient and health systems perspectives) as well as consideration of the skillsets required to deliver the applications.³

Policy Context and Recent Developments

Two recent OECD workshops concluded that mHealth is by far the fastest growing segment of IT-based healthcare delivery systems. These technologies offer a wide range of smart modalities through which patients can interact with health professionals or systems. MHealth technologies do this by providing helpful real-time feedback along the care continuum, from prevention to diagnosis, treatment and monitoring. Since 2008, the Group Social Mobile Association (GSMA) has tracked over 1,200 mHealth deployments globally. Furthermore, in 2015 alone, over 116 case studies of digital health deployments were reported in USAID’s annual mHealth Compendium. Reports from the first quarter of 2014 show that there were about 100000 mHealth apps listed in the two major app stores (Apple and Android). Moreover, the annual revenue of the health-related mobile apps market is projected to reach more than USD 26 billion (USD) by 2017 from its value of USD2.4 billion in 2013.³

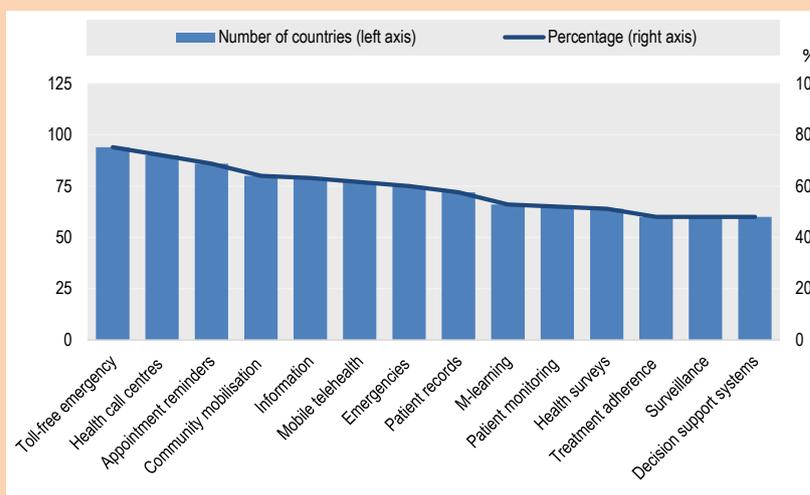
¹ WHO (2011) MHealth: New horizons for health through mobile technologies
http://www.who.int/goe/publications/goe_mhealth_web.pdf

² Consulting VW. mHealth for Development: The Opportunity of Mobile Technology for Healthcare in the Developing World. 2009; WHO. mHealth New horizons for health through mobile technologies. Global Observatory for eHealth series 2011;3. http://www.who.int/goe/publications/goe_mhealth_web.pdf

³ World Bank – (2011) ICT Sector Unit Mobile Applications for the Health Sector 2011; The Boston Consulting Group. The Socio-Economic Impact of Mobile Health. 2012.; Iain B Labrique LV, Erica Kochi, Robert Fabricant, Garrett Mehl. mHealth innovations as health system strengthening tools: 12 common applications and a visual framework. Global Health: Science and Practice 2013;1:160-71.; WHO. WHO mHealth Technical and Evidence Review Group (mTERG) for reproductive, maternal, newborn and child health.

In 2015, WHO surveyed over 125 countries on eHealth and mHealth activities at the national level. Over 80% of these countries reported government-sponsored mHealth programs. MHealth projects primarily extended existing health programs and services at the national or local level (as opposed to international) (Figure 1).

Figure 1. Adoption of MHealth Programme by Type (2015)



Note: The results include responses from over 600 e-health experts in 125 countries worldwide. Source: World Health Organization (2016), Atlas of eHealth Country Profiles: The Use of eHealth in Support of Universal Health Coverage: Based on the Findings of the Third Global Survey on eHealth 2015, http://apps.who.int/iris/bitstream/10665/204523/1/9789241565219_eng.pdf?ua=1.

Government engagement was primarily guided by eHealth and telehealth policies (60% of responding countries); and no specific policy guidance was reported for mHealth in 30% of countries. Over half of countries actively provided policy guidance on standards, privacy and/or security. Policy gaps included policies on data ownership, regulation of devices, oversight of mobile health apps and evaluation. Across survey responses, there was notable regional variation in the enabling environment.

A particular focus of recent mHealth policy debates revolves around data privacy and security. With the increased ability to collect large amounts of personal data over space and time comes greater risk of personal information breaches that threaten to erode consumer trust in sharing personal data from mobile and web sources. Uncertainty is amplified by the persistent threat of theft and hacking and the increased ability to re-identify data. Based on the information reported in the United States Department of Health and Human Services (“HHS”) Office of Civil Rights (“OCR”) database, which publishes the breaches affecting 500 or more individuals, approximately 112 million Americans or nearly one third of the United States population had been affected by breaches of “protected health information” (“PHI”) in 2015.⁴

The default position, in the context of uncertainty, is often to restrict collection and use of personal data (health and other data - including geolocation data). However, mHealth growth may be stymied by such an approach. It is therefore critical to promote policies that weigh the trade-offs through an assessment of the individual risk against the benefits (individual and social), taking account of the likelihood and impact of each.

Closely related to concerns about data privacy is the concept of trust and how to operationalize it in national policies. Any policy efforts to support and maintain trust must clarify a) what trust means in the mHealth context; and b) the links between trust and trustworthiness.

- **Trust** is the state of mind that enables a person to be willing to make herself vulnerable to another in seeking health care and when participating in health-related research. Trust relationships in health information systems may operate one-on-one, locally to a specific organization, or across institutional boundaries. In mHealth, the trustor to trustee relationship may involve any combination of individuals, organizations, institutions, or systems. Examples include the doctor-patient relationship, the relationship between consumers and a provider organization or an app vendor or a research university, and the relationships defined by agreements between user and service suppliers.
- While trust is an attitude towards mHealth, **trustworthiness** is a property of mHealth. Trustworthiness can be defined as a number of specific features, characteristics, attributes, etc. that render mHealth applications and systems worthy of trust. Often trust and trustworthiness are conflated. However, to reach the goal of inspiring and maintaining trust, it is imperative to develop trustworthy mHealth systems. Governance frameworks must spell out the norms and measurements that can ensure trustworthiness.

The Need for Integrated Approaches in Promoting Trust

Countries are seeking to promote a strong “fabric of trust” between stakeholders, including the general public, to assure the good intentions of data sharing for individuals, organizations, and institutions in providing health care services and conducting research. While links between consumer trust, privacy and security have long been clear, they have traditionally been addressed in silos. This creates a need for integrated approaches in managing consumer/patient protection, privacy, security, and safety risks. Factors for consideration include:

- **Privacy, security and data protection:** Data privacy is an important factor affecting willingness to use services and share personal health data. Privacy is notoriously difficult to define, but commonly refers to individual control of how, when, what, and to whom information about one’s self is revealed. *From the privacy point of view*, trust is about the willingness of an individual to become vulnerable to an organisation by disclosing personal data. A “trustworthy service provider or organisation” ensures privacy is protected according to laws and regulations and by taking several measures: e.g. is transparent about the data gathered and the intended uses, offers choices with respect to information disclosure and whether and how personal information is used, , respects the conditions of data use that have been set by individuals, and should be able to ensure the security of the collected data by taking reasonable steps to guard against loss or misuse of personal information provided by consumers.
- **Value and use:** For individuals to be willing to give up some privacy and control over their data, they ultimately need to decide if benefits outweigh costs. Willingness of individuals to share personal health data has been demonstrated to be strongly linked to the question of what that data will be used for, and in particular to the value of that use. Research has shown that some individuals are more willing to share their data if it will directly benefit them, while others may be motivated by altruistic reasons.⁴
- **Control and ownership:** This is a gray area in the mHealth space. Many believe that consumers themselves have complete control over the data on their devices. This is not always the case. In order to access a service, consumers regularly are asked to agree to have their data shared with a number of parties via their devices’ privacy policies, terms and conditions, and user agreements. Given the many actors in the mHealth ecosystem, it has become increasingly difficult for users to monitor or control data utilization, let alone “own”, their data. Informed consent generally presumes the ability to indicate clearly to the user/consumer the use and purpose of the particular data collection activity. The ease by which multiple data from diverse devices and sources can now be collected, stored, analysed and shared in greater volumes than ever before renders the provision of this type of information particularly difficult. In

⁴ Moore D and Niemi M (2016) The sharing of personal health data- A review of the literature- Sapere Research Group

addition, mHealth data can be used for numerous purposes that may be unknown at the point or time of collection, which makes the implementation of informed consent difficult.

- **Transparency and accountability:** Accountability is key for consumer trust and more so when personal data is collected and used at a distance from the individual. Considering the multiplicity of parties involved in the mHealth industry and the different role played by each, it can be difficult to identify all controllers and processors and ensure an appropriate allocation of responsibilities. As such, transparency is critical to help promote accountability of all relevant actors.
- **Quality and safety:** These dimensions are important features that play directly into consumer/user and care provider trust. From a health perspective, safety may mean that the mHealth system produces information that is valid and of adequate quality for critical decision-making. For example, given the rapid onset of a heart failure event and the potentially catastrophic impact of a missed detection, an mHealth system that predicts heart failure in patients with congestive heart disease must maintain high-quality information continuously over an extended time period. From an engineering perspective, safety might mean that devices, such as sensors, used in mHealth systems do not cause their users unanticipated harm because of design or manufacturing errors. Data collection using mHealth sensing may also introduce various data quality and associated safety challenges. Poor data quality could result in suboptimal outcomes, including missed opportunities for effective intervention or even wrong information to improperly guide health decisions.

As countries wrestle with how to integrate these dimensions into their mHealth policies, a range of organizations has sought to inform and support such efforts. Examples include recent reviews in the United States by regulatory agencies such as the Office of the National Coordinator for Health Information Technology (ONC), the Food and Drug Administration (FDA) and the Federal Trade Commission (FTC); in Europe, the European Commission (EC) developed a Green Paper on mHealth (2014) and the European Data Protection Supervisor (EDPS) issued an Opinion clarifying how the new European General Data Protection Regulation (GDPR, 2015), which will come into effect in Europe in 2018 and applies to mHealth. One of the aims of the GDPR is to strengthen the rights of the data subjects, particularly in situations where interference with their right to privacy might be magnified by online interaction. The GDPR also introduces new guiding principles and rules applicable in the context of mHealth. For example, privacy by design and by default become legal obligations (and no longer mere "best practices") under the GDPR, and thus will have to be fully taken into consideration when designing new mHealth apps or devices.

The OECD adopted a Recommendation on Health Data Governance in January 2017 that provides high-level policy guidance to encourage the availability and use of personal information and promote its use for purposes that serve health-related public interest. These efforts make clear that regulation is evolving and, in turn, that regulation is necessary but not sufficient to harness the potential of mHealth. While regulatory developments are ongoing, there is increasing understanding that regulation will be only one element in the effort to realize the potential of mHealth while preserving ethical and social values. Ensuring the appropriate governance framework for mHealth will therefore require a number of components beyond legal instruments for data protection.

GLOBAL EXPERIENCES WITH MHEALTH AND ASSOCIATED POLICY CHALLENGES

To inform discussions related to policy needs, the conference included national and regional examples of specific mHealth efforts. These presentations provided an opportunity to examine, in some detail, the direction and challenges of mHealth efforts in both low and high income countries. The following case studies were selected because they reveal specific domains of particular relevance to public health interventions in low income countries and where a fundamental shift is urgently needed in the delivery of health care (e.g., to meet the health needs of older populations) . The examples also highlight key policy challenges in the broad and evolving field of mHealth as well how technologies developed to solve problems in developing countries may also be useful in high-income countries especially in remote regions and for vulnerable populations (reverse innovation).

Using Mobile Phone Data to Model and Predict the Spread of Infectious Diseases

Accurate information on population movements is valuable for monitoring the progression of an outbreak and predicting its future spread, facilitating the prioritization of interventions and designing surveillance and containment strategies. Vital questions include how the affected regions are connected by population flows, which areas are major mobility hubs, what types of movement typologies exist in the region, and how all of these factors are changing as people react to the outbreak and movement restrictions are implemented.

Just a decade ago, obtaining detailed and comprehensive data to answer such questions over large geographical regions would have been impossible. Today, such valuable data exist and are collected in real-time, but largely remain unused for public health purposes – stored on the servers of mobile phone operators. Mobile phone networks, also called cellular networks, are composed of cells, i.e. geographic zones around a phone tower. Each communication can be located by identifying the geographic coordinates of its transmitting tower and the associated cell. Mobile call data records (CDRs) detailing the time and associated cell tower of calls and text messages from anonymous users therefore provide a valuable indicator of human presence, and sequences of these data can be used to measure population movements over time, especially when existing mobility data is poor. With network operators serving substantial portions of the population across entire nations, the movements of millions of people at fine spatial and temporal scales can be measured in near real-time and can provide useful information on trends and fluctuations over time helping to reduce uncertainties attached to outbreak detection and response. Flowminder (Box 1) offers an example.

Despite the value of CDRs, mobile network data is generally very difficult to access due to commercial and privacy concerns. In particular, extending geolocation data to the management of natural disasters or outbreaks entails the problem of the nature of the information—often private and/or sensitive— associated with them. It is, therefore, important to be especially aware of issues relating to security and privacy in order to make use of geolocation tools responsibly. De-Montjoye has recently shown, for example, that four spatio-temporal points may be enough to uniquely identify 95% of people in a mobile phone database of 1.5M people and to identify 90% of people in a credit card database of one million people.⁵ While these results may not be definitive, this work does raise key policy questions on how best to gain access and realize the public health benefits of CDRs while also protecting privacy. A promising model moving forward relies on pseudonymous data through secure and auditable question and answer systems⁵. However, there are additional issues that need to be considered such as possible bias due to the potential heterogeneity and poor verifiability of the data collected. Open-access to the data collected and the metadata as in the case of Flowminder is thus critical to allow for validation and ensure transparency

⁵ <http://opalproject.org/> and <http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0098790>

Box 1. Flowminder

Flowminder is a non-profit foundation working with data providers and international/government agencies to operationalize and scale applications in support of vulnerable populations and sustainable development. The organization uses mobile operator data, which is anonymized on a server hosted by the cell operator. Flowminder conducts analyses on this data under operator supervision with raw data anonymized behind an operator firewall. As such, the organization is able to preserve user privacy, as the data never leaves the mobile operators system. Aggregated data can then be exported and made open access, to be paired with epidemiological data and other information. Uses of the application include measuring population data and migration, disaster response and preparedness, and infectious disease modeling.⁶ In an effort to allow for validation and ensure transparency, and to expand the utility of the data sets and predicted mobility patterns, where possible flowminder makes geographic, population, and mobility data as well as methods openly available.

This application is an example of how to leverage the rising prevalence of routine cell phone use to advance public health. As disasters cause large-scale population movements, Flowminder has been used to map where people are moving during a disaster and predict population displacement and other consequences after a disaster. One example is the Nepal Earthquake. Prior to the earthquake, Flowminder and Ncell (the largest mobile operator in Nepal) began a collaboration to respond to potential future earthquakes in Nepal. In the aftermath of the earthquake, it was immediately apparent that there was a mass population movement, initially as the result of people fleeing affected areas. Large numbers of people also moved to sleep in safer, open areas after losing their houses or due to fear of aftershocks.

Understanding where affected people are located is essential for effective humanitarian response. The WorldPop project mapping team rapidly produced population density maps. These data were used by UN OCHA and other agencies to estimate the number of people affected. The Flowminder and WorldPop mobile analysis team then used these population data in combination with the Ncell anonymised data from 12 million mobile phones in Nepal to quantify the impact of the earthquake on population movements. After adjusting for normal population movement patterns, which would have occurred in the absence of the earthquake, the Flowminder analysis showed that an estimated additional 500,000 people had left Kathmandu two weeks after the earthquake. The majority of these went to the districts surrounding Kathmandu and to the Terai areas in the south and south-east of Nepal, was previously completely unknown. Flowminder is now working with key organizations to ensure that the capacity to respond with similar analyses in future earthquakes and disasters can be maintained, as well as planning for the implementation of several analysis products to support development and public health in Nepal going forward.

Connected Health Delivery System for Remote Care in Korea

Challenges associated with supporting and caring for ageing populations are impacting both high and low income countries. As outlined in the 2015 WHO World Report on Ageing and Health, and reported by the Commonwealth Fund, older people with chronic disease in all countries face care coordination and safety problems and are not accessing care in the numbers we would expect.² Thus, a particular focus of high-income countries is how to extend traditional healthcare services to older populations in their home setting as well as to those living in remote areas and improve care coordination.

In Korea, these issues have motivated efforts to apply mobile technologies for remote care. However, as with other countries, issues of reimbursement impeded progress. Without adequate reimbursement, providers have a strong disincentive to invest in mobile technologies. The Korean UHealth project (Box 2) offers an example. Given the

benefits inherent in the deployment of mobile technologies to extend access to the traditional healthcare delivery system, particularly for remote care and care for home-bound elderly patients, it is in the interest of payers to help health care providers finance the switch to these technologies because of the benefits that would accrue both to themselves and to the people on whose behalf they purchase health care. Recent regulatory developments in telehealth reveal how public policies and changes in reimbursement scheme have helped to better integrate the use of telehealth services into mainstream health care in a number of countries. To date, however, there is still no universal consensus on criteria for telehealth reimbursement as well as for mHealth in general. Countries therefore need to fully analyse the benefits of remote care services and, where needed, revise their payment models to pave the way for effective implementation and adoption of mHealth.

Box 2. UHealth in Korea

UHealth is a healthcare demonstration project is a public-private partnership funded principally by the Korean Ministry of Health and Welfare focusing on pre-care and wellness. The UHealth program involves monitoring a patient's vital signs and other critical health information virtually anywhere. This can include blood pressure, blood sugar, body weight, cholesterol levels and ECGs. Monitoring can also include physical activity, exercise, nutritional intake and other lifestyle information that might be relevant to an individual's health. The UHealth demonstration project includes a number of projects today mainly focused on creating foundational components, such as: core technologies, standardization, communications, and equipment to support UHealth environments and services.

The greatest challenge to the program's success is not the technology or even the infrastructure rather regulatory uncertainty-in particular the issue of reimbursement and liability.⁷

Source: J. Park, Harvard Global Health Institute Workshop (2016)

MHealth Solutions for Improved Maternal and Newborn Care

Low-income countries face a variety of obstacles to improved reproductive, maternal, newborn, child and adolescent health (RMNCAH): cost-effective mHealth interventions have been shown to dramatically reduce maternal mortality in certain cases. As an illustration, over the past 20 years, the Latin American and Caribbean countries region has made significant advances in improving maternal health and mortality rates have fallen over 40%. National averages often mask, however, local inequalities. Although Latin America had a maternal mortality ratio of 77 maternal deaths per 100 000 live births in 2013,⁸ these same ratios are 10-44 times higher in the poorest provinces of several countries in Latin America. Latin America and the Caribbean have also made slow progress in reducing adolescent childbearing, with the adolescent birth rate remaining high, at 73 births per 1000 girls in 2015⁹.

MHealth can play an essential role in supporting strategies to reduce maternal and child mortality, delivering information, facilitating access to care and enabling evaluation to better deliver timely resources. For many of these projects, however, once the initial funding runs out, a significant challenge is developing a sustainable business model, regulatory barriers and sustained political support, among others. As such, long-term sustainability and financing appear to be the most challenging obstacles, and, in most cases, poorly-understood aspects of mHealth initiatives. In other words, often the focus is the technical feasibility of the project and achieving successful adoption, with the economics and politics of the approach playing a secondary role. Ultimately, however, it is the value to society and political will that will determine whether a given project might survive or not. TulaSalud (Box 3) offers an example.

There is no magic bullet today with respect to the options or strategies required to achieve economies of scale and long-term financial sustainability. Many initiatives are still struggling to begin exchanging health information, whereas the more mature initiatives face challenges about how to expand their services in a financially sustainable

way. Financial sustainability is a critical issue for all initiatives, even those that are relatively more mature and directly funded by government, and stands out as a persistent concern.

Box 3. TulaSalud: Equipping Rural Community Health Workers

TulaSalud is a Guatemalan non-governmental organization, whose purpose is to support the Ministry of Public Health and Social Assistance of Guatemala and partner institutions to improve rural health services. Specifically, TulaSalud works to reduce maternal and infant morbidity and mortality, malnutrition, and other programs that are aimed at improving the access of health services to the most needy rural population in Guatemala. The project began in 2004, through a bilateral agreement between the Canadian government and the government of Guatemala. The main objective of the project was to increase the number of nursing staff in rural and postponed areas of the country. As a result, it began with a pilot course that trained 34 nursing assistants from indigenous and rural communities in Alta Verapaz, using Optel Tele-Writer technology for distance education.

TulaSalud has since broadened in scope and now focuses on Community Facilitators (CFs), a volunteer accepted by the community who, with a small stipend from the Government, who provides basic primary care services. The innovation introduced by TulaSalud during the implementation of this program has been to provide CFs with cell phones that allow them to: Consult with healthcare specialists, provide full epidemiological and clinical information relating to the patients they attend (using Kawok, which is based on CommCare) and coordinate patient transfers in case of emergency. Cell phones also enable CFs to receive ongoing training through audio-conferences. They also allow to carry out health promotion and prevention activities with the population via remote briefings in the Q'eqchi' or Poqomchí languages. Currently 195 community tele-facilitators cover 710 communities and a population of approximately 330.000 people.

In 2011 TulaSalud started to collaborate with the EHAS (Enlase Hispano Americano de Salud) Foundation, a Spanish NGO whose mission is to promote affordable and innovative uses of ICT to improve the public healthcare delivery in remote areas of developing countries. EHAS is currently supporting the Healthy Pregnancy initiative, which aims to reduce maternal mortality rates in rural areas.

Source: I. Prieto-Egido, OECD-Harvard Global Health Institute Workshop (2016)

MHealth for Better Adherence to Therapeutic Guidelines and Protocols in Low Resource Settings

Many low resource settings have weak health systems characterized by poor physical and ICT infrastructure, inadequate and poorly trained health workers, weak policies and organizational capacity, and inadequate financial investment (including data systems). eHealth/Health IT and mHealth have been shown to enhance quality of health care through better adherence to therapeutic guidelines and protocols, informing clinical decisions, and decreasing medication errors. In particular, there is now good evidence that mHealth tools can improve detection, linkage to care, retention in care, and adherence to Anti Retro Viral therapy (ARVs) in HIV patients.

As an illustration, two recent randomized trials in Kenya have evaluated the benefits of using weekly interactive text messages reminders to improve adherence to antiretroviral therapy (ART). The first trial reported improvements in adherence and viral load,¹¹ a second reported an improvement in adherence and a reduction in treatment interruptions.¹² In a form of reverse innovation, this same service (WelTel) has since been applied among populations with HIV and latent tuberculosis in British Columbia (Canada), and to improve latent tuberculosis medication completion and in providing support to Aboriginal Canadian youth and high-risk HIV patients.

In South Africa, SMS text messages have also been used to improve HIV health care service delivery by improving communication between patients and health personnel, and also as an appointment reminder.¹⁰ There remain, however, some critical challenges in implementing mHealth in low resource settings which include the following:

- Human Capacity:
 - Although varied from one country to another, capacity is still limited for the development of high quality mHealth solutions.
 - Inadequate training of end-users, including health care workers.
- Infrastructure:
 - Limited cellular coverage in rural areas where majority of vulnerable populations live. Slow connection. Signal outages.
 - Unreliable/unavailable electric power to keep devices powered (e.g. SMS printers).
- Costs:
 - Relatively high cost of data bundles for smart phones, and text or voice calls for basic handsets.
- Legislation, Policies and Standards:
 - Lack of appropriate legislation to support the integration and scaling of mHealth into mainstream health care services.
 - Limited regulatory oversight based on policies and standards to guide quality and safety:
 - Sub-standard mHealth products → wrong clinical or public health decisions → compromised patient safety, quality of care, incorrect public health inference.
- Inadequate evidence on what works at scale

Box 4. Implementing MHealth for the management of HIV in sub-Saharan Africa

At the end of 2014, 10.7 million people living with HIV in sub-Saharan Africa were receiving antiretroviral therapy (ARVs)—roughly 72% of the 14.9 million people receiving ARV globally. First-line ARV regimens comprise the standardised efficacious, cost-effective, widely available, and least toxic drugs. The consequences of ARV failure include increased risk of HIV-associated complications, such as opportunistic infections, malignant diseases, and neurocognitive dysfunction.

Studies done in sub-Saharan Africa in 2014 showed that 15–25% of people receiving ARV experienced conditions that define treatment failure. In 2014, ~69% of the adult population in Africa also owned a mobile phone, which can be an effective means¹³ to extend health care services to rural and hard-to-reach areas (e.g. informal settlements/slums) where the most vulnerable and under-served populations live. The research literature provides evidence on a range of interventions, which might contribute to the ways in which mHealth for HIV might facilitate the scale-up of HIV prevention, care, and treatment services.

First, mHealth tools can be used to increase testing among vulnerable communities. For example, Welz and Herbst¹⁴ describe the use of handheld computers for delivering HIV testing results in hard-to-reach South African communities. Mhealth tools can also be used to promote adherence. Use of mHealth to improve adherence has the strongest evidence base to date. The most commonly documented use of mHealth is 1-way text-message and phone reminders to encourage follow-up appointments, healthy behaviors, and data gathering. Several descriptive and quasi-experimental studies suggest that text message reminders are acceptable, feasible, and useful for improved treatment adherence.¹³

Sources: R. Lester and T Olouch, OECD-Harvard Global Health Institute Workshop (2016)

FRAMEWORKS AND TOOLKITS TO SUPPORT MHEALTH ADOPTION AND SCALING

There is now an established and growing body of literature on the importance of priority setting, resource allocation and benchmarking in the adoption of information technology in healthcare. Methods of priority setting that use explicitly defined criteria can aid health care decision makers in arriving at funding decisions in a transparent and systematic way. However, we know little about why and how healthcare organisations reach decisions on mHealth. It is thus important to identify and examine what evaluation frameworks have been used to categorize and prioritize mHealth interventions to date. As an illustration, the next sections review the framework developed by the World Health Organisation (WHO) Department of Reproductive Health and Research (RHR) to assist government-led investments of digital health strategies for strengthening reproductive, maternal, newborn, child and adolescent health interventions. It also reviews complementary work on eHealth governance and policy frameworks that could be extended to mHealth.

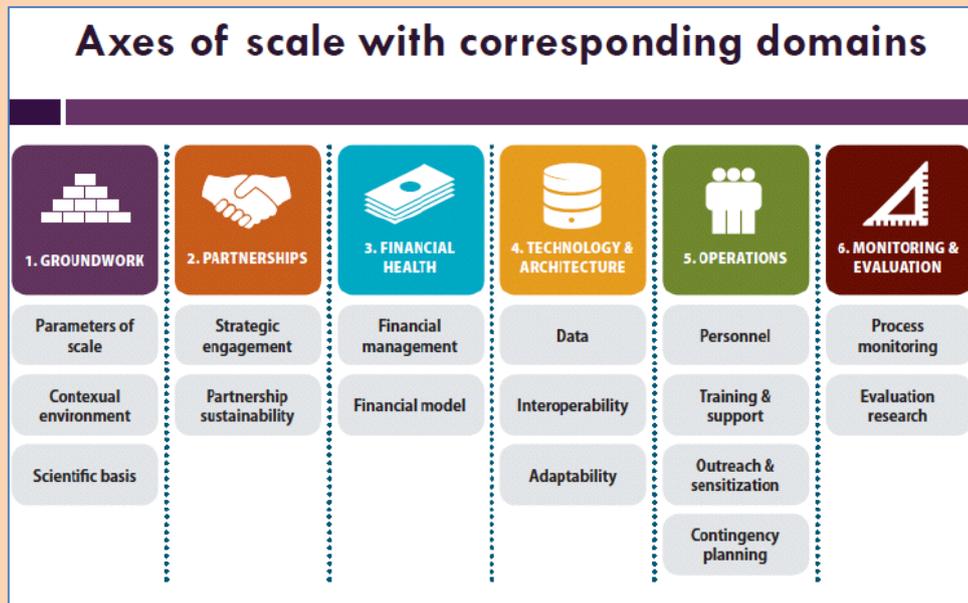
The WHO MHealth Assessment and Planning for Scale Toolkit

The WHO mHealth Assessment and Planning for Scale (MAPS) toolkit has two overarching goals – to assist and to plan. The toolkit assists mHealth project teams to critically assess their mHealth project as they move from piloting to planning their next steps for overcoming the challenges inherent in scaling up. The Toolkit guides mHealth projects through a continuous process of thorough assessment, careful planning, and targeted improvements.

The Toolkit's aim is to shift the assessment from whether the mHealth initiative “works” to process evaluation or proxy indicators of the health outcome(s) of interest. Questions include: when should mHealth be applied along the care continuum (e.g. to strengthen health promotion and prevention; what health interventions are enhanced by the application of mHealth (e.g., to promote reduced salt intake); which health system constraints are being overcome (e.g. to address low availability for specific services); how mHealth is applied (e.g. the technology used); where MHealth engages actors (e.g., if the service targets with an sms the patient’s phone). This approach is meant to facilitate the selection of mHealth tools that are appropriate for identified policy or systems-level challenges. In other words, it would drive people to first identify key obstacles, or constraints, to delivering proven health interventions effectively, and to then apply appropriate mHealth strategies that could overcome these constraints and scale successfully.

It lays out six overarching thematic areas designed to provide actionable information on mHealth deployments. These six areas, also known as axes, are: Groundwork, Partnerships, Financial health, Technology and Architecture, Operations, and Monitoring and Evaluation. Each of the six axes contains a set of structured self-administered questionnaires and scorecards that enable mHealth project teams to objectively measure their progress in relation to implementation, the potential for scaling up and ensuring sustainability (Figure 2). Each axis also includes tips and lessons from the field – all informed by the experiences of pioneering mHealth projects.¹⁵

Figure 1. Axes providing project information



Source: M. Orton, OECD-Harvard Global Health Institute Workshop (2016)

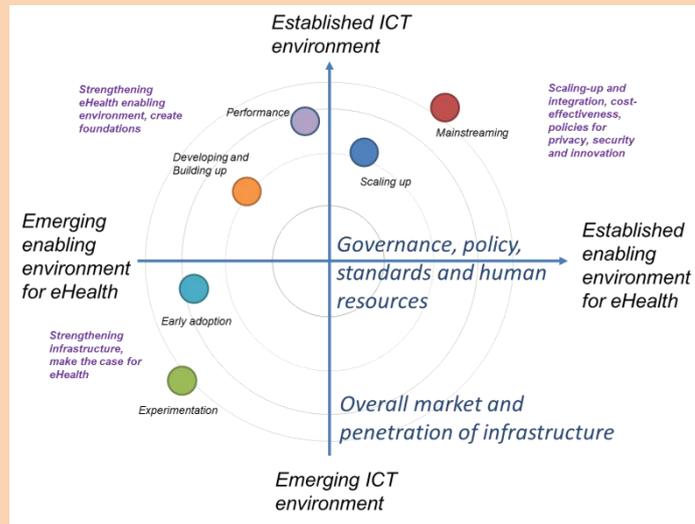
Identifying Dimensions of Foundational MHealth Policies

Complementary WHO efforts explicitly target needed domains of eHealth governance and policy that can be applied to mHealth. Specifically, the WHO/ITU National eHealth Strategy Toolkit¹⁶ can be used to ensure that foundational/enabling policy frameworks are in place and can support mHealth policy efforts. The Toolkit identifies seven essential components. These are the following: i) leadership and governance; ii) strategy and investment; iii) services and applications; iv) standards and interoperability; v) infrastructure; vi) legislation policy and compliance; vi) workforce. An accompanying maturity model (Figure 3) could readily be adapted to mHealth specific needs, but this has not yet occurred. As a first step, the model recommends that a national vision for Mhealth implementation should align with the country's health priorities, as well as with the existing infrastructure capacity.

A detailed action plan and a monitoring and evaluation framework can then address fundamental issues such as regulation, governance, standards and interoperability, workforce and financing.

The case studies in the previous sections demonstrate that an MHealth implementation plan, if built on health priorities and in coordination between authorities (e.g., Ministry of Health, Ministry of Communication), and private sector (e.g. telecom operators and app developers), can facilitate the development of common policies and standards and thereby support data interoperability across systems and programs. Mhealth is at the intersection of a number of sectors and as a result requires leadership, expertise and investments from all major stakeholders.

Figure 2. eHealth Maturity Model



Source: J. Dzenowagis, OECD-Harvard Global Health Institute Workshop (2016)

APPROACHES TO THE EVALUATION OF SAFETY, EFFECTIVENESS, AND PRIVACY PROTECTION OF MHEALTH “APPS”

In developing countries, the number of mobile-broadband subscriptions per 100 inhabitants reached in 2016 a penetration rate of close to 41% while in developed countries it was 90%. Over a third of the world's population is thus today -at least in principle- using a mobile device to access the Internet and capable of supporting apps. Apps are generally understood as a category of software developed to run on mobile platforms for a single or limited number of purposes. However, the distinction between apps and other software applications has become less clear as a wider range of computing platforms support apps and app repositories, and as apps with a wider range of functions are developed. Mobile health and wellness apps come in a variety of forms, each with their own unique purpose. There are two broad categories into which these apps fall (although the distinction is not always straightforward): (a) apps for the purpose of prevention, diagnosis and treatment of diseases (medical apps); and (b) apps relevant to lifestyle, fitness and well-being (nonmedical apps). Among the former, the integration of apps and their ability to track data in the outpatient setting is playing an integral role in the rise of remote care including telemedicine activities. Recent research for example indicates that apps targeting individuals with chronic illnesses are likely to be useful in patient engagement efforts.

Among the latter, besides lifestyle and fitness apps, many organizations and hospitals are investing in apps to serve as patient education tools, incorporating videos and touch-based teaching methods. Additionally, mobile apps are being used in the education of medical students through the use of quizzes and virtual flashcards. They are also being utilized as digital simulations of clinical situations or surgical interventions, taking advantage of the touch-based display on the smart device. In addition to mobile apps functioning as standalone elements, mobile apps are increasingly integrating with other peripheral devices.

Mobile health and wellness apps thus comprise a significant segment of the app universe. In consumer surveys, a quarter of US adults reported in 2014 using one or more health tracking apps and a third of physicians had recommended an app to a patient in 2013.¹⁷ The combination of the rapidly evolving apps and app platforms and integration with other products introduces new opportunities as well as possible new risks. In particular there are persisting questions about:

- Clinical effectiveness and safety
- Privacy and security (Many health and fitness apps have access to sensitive, physiological data collected by sensors on a mobile phone, wearable, or other device)
- High rate of app turnover (Nearly 90% apps are not used after six months; 80% are not generating revenue to support a business case)

Recent research also shows that while consumers are faced with a wide choice of apps addressing a broad set of medical conditions, a minority of these apps are likely to be useful for improving health.¹⁸ Frameworks that consider the engagement, quality, and safety of mobile apps are thus critically needed to assist and guide consumers in identifying trustworthy apps that serve their specific health and wellness needs. An example of key questions (as developed and validated by the NHS) may be relevant for adaptation to other contexts. The NHS's process is based on ten thematic areas that contain 80+ questions in total. The answers to these questions are used to generate a report for app developers, which can be used to assess if their apps meet the NHS' standards. Because questions are answered by developers, the process will be subject to audit. This effort is still in process and is meant to provide a benchmark for the quality of app development in healthcare. Sample questions in four of the ten thematic areas include:

- Privacy & Security: Are you looking after information in line with the Data Protection Act and protecting personal data in line with best practice?
- Equality: What efforts have been made to make your App available and usable by the widest number of people?
- Safety: What risk could your app pose and how is that risk communicated and managed?

Effectiveness: What efforts and evidence can you provide to support the effectiveness of your app?

The MHealth App Regulatory Environment

In some countries regulation on medical devices apply today to a subset of high-risk mobile medical apps. In Europe the CE certification process for medical devices sets the requirements for health apps that qualify as medical devices. The MEDDEV 2.1/6 "Guidelines on the qualification and classification of standalone software used in healthcare within the regulatory framework of medical devices" provide some guidance for developers on which apps qualify and which do not- as this is not easy to assess. In 2015, the United States Federal Food, Drug Administration issued a similar Guidance on 'Mobile Medical Applications' (Mobile Medical App) setting the requirements for mobile apps that meet the definition of a device under section 201(h) of the Federal Food, Drug, and Cosmetic Act (FD&C Act). According to this Guidance, an app is considered a medical device if it:

- Is an extension of one or more medical devices by connecting to such device(s) for purposes of controlling the device(s) or for use in active patient monitoring or analysing medical device data.
- Transforms the mobile platform into a regulated medical device by using attachments, display screens, or sensors or by including functionalities similar to those of currently regulated medical devices. Mobile apps that use attachments, display screens, sensors or other such similar components to transform a mobile platform into a regulated medical device are required to comply with the device classification associated with the transformed platform.
- Becomes a regulated medical device (software) by performing patient-specific analysis and providing patient-specific diagnosis, or treatment recommendations. These types of mobile medical apps are similar to or perform the same function as those types of software devices that have been previously cleared or approved.

Many of the health and wellness apps on the market are not considered medical devices and are therefore not subject to specific evaluation. As such, it is imperative that individual users understand how to critically appraise and properly identify health and wellness apps that are safe to use. A number of emerging initiatives aim to fill the evaluation gap. For example, medical app accreditation programs, in which apps are subject to formal assessment or peer review, are a recent development that aims to provide clinical assurances about quality and safety, foster trust, and promote app adoption by patients and professionals.^{19,20} Voluntary codes of conducts or codes of practice are also being developed to promote private sector awareness and good practice (see Box 5).

While not yet integrated into a single framework, several academic-led efforts have also sought to contribute to health and wellness "apps" evaluation. These efforts provide early evidence on possible key challenges as well as quality assurance criteria that should guide evaluation. A recent study for example assessed the extent to which 79 already-certified apps complied with data protection principles mandated by a prominent national accreditation program; the English National Health Service (NHS) Health Apps Library.¹⁹ Launched as a pilot project in March 2013, the NHS Health Apps Library's aim was to provide a curated list of apps for patient and public use. In respect of privacy, the accreditation approach adopted by the NHS Health Apps Library was to require developers to declare any data transmissions made by their app and, in this case, to provide evidence of registration with the Information Commissioner's Office (ICO), the UK body responsible for enforcement of the Data Protection Act (information

obtained via Freedom of Information request). Registration entails a commitment to uphold principles of data protection and is a requirement under the Act for individuals or organizations processing personal information.

Thus, while substantially relying on self-declaration, it is clear the expected intent, and the assumption that might reasonably be made by app users, is that apps accredited by the NHS Health Apps Library will comply with UK data protection principles concerning information privacy. The study found that while two-thirds (67 %) of apps had some form of privacy policy; 66% of the apps sent identifying information over the Internet without encryption; 29% of apps sent strong identifying information without encryption (including email addresses, account login details, full name or date of birth); and half of apps transmitting user account details sent usernames and passwords unencrypted.²¹ A sixth of apps sent information to advertisers and third-party analytics but did not mention secondary uses of information in their policy.

Many of the privacy issues identified are addressed by best-practice guidelines targeting developers. The findings however highlight potential shortcomings of a voluntary accreditation approach that, in respect of privacy at least, appeared to rely mainly on self-declared compliance.

Similar shortcomings have recently been reported in a study focusing on the safety and effectiveness of 46 insulin dosing smartphone apps. The study found that 44/46 (95%) apps had issues affecting data input; 14/46 (30%) apps listed the formula used to suggest an insulin dose; 42/46 (91%) apps did not apply validation to all numeric inputs; 22/46 (48%) of apps used ambiguous terminology to label and describe inputs; 31/46 (67%) of apps risked displaying an incorrect or inappropriate result despite inputs being configured correctly; 22/46 (48%) apps violated basic clinical assumptions; and only one app was issue-free.²¹

These studies uncover an urgent need for internationally agreed quality assurance and evaluation criteria that can adapt to changes in technology, address data governance-related risks, ensure robust digital risk management and compliance with medical evidence base and reflect local variations in clinical practice.

Box 5. Ongoing EU-level activities related to mHealth apps

There is no EU-wide guidance below the so-called 'medical device level' for health apps, other than general consumer protection requirements as provided under the Consumer Rights Directive, Ecommerce Directive and Unfair Commercial Practices Directive.

To address this uncertainty, ongoing EU-level voluntary activities in relation to mHealth apps today include:

- the code of conduct (CoC) for mHealth app developers formally submitted for comments to the Article 29 Data Protection Working Party at the beginning of June 2016; The CoC, aims to provide easily understandable guidelines for app developers on how to respect (and comply with) EU data protection rules. Although voluntary, once certified entities will be legally required to respect the requirements set out under the CoC. The code is a voluntary instrument and will require interested parties to certify, meet and respect the obligations.

- the EU-wide PAS 277:2015 Health and wellness apps – Quality criteria across the life cycle – Code of practice ('PAS277')² standard, which was developed by the British Standards Institution ('BSI'); and -the international Standard IEC 82304-1, published in October 2016 and prepared by a Joint Working Group of IEC subcommittee 62A (Common aspects of electrical equipment used in medical practice) and ISO technical committee 215: Health Informatics [<https://www.iso.org/standard/59543.html>] . The primary focus of the standard is on the requirements for manufacturers. It covers the entire lifecycle including design, development, validation, installation, maintenance, and disposal of health software products.

- MHealth Assessment Guidelines- these voluntary Guidelines aim to build on existing initiatives and best practices from across Europe and beyond. They propose a set of nine common criteria (Usability & accessibility; Desirability;; Credibility; Transparency; Reliability; Technical stability; Safety; Effectiveness; Privacy & security) to help different stakeholders including end users, developers, payers of care, and vendors of electronic health record systems to assess the validity and reliability of mHealth apps.

In addition to the above, the European commission ran a public consultation on the safety of apps and other non-embedded software between 9 June and 15 September 2016. The consultation gathered a total of 78 replies from stakeholders in EU Member States as well as from outside the European Union. Across all stakeholder groups that responded, health and wellbeing apps were identified as the main category of apps that could pose safety risks. For some private sector respondents, most of the safety risks exist in the so called "grey zone", where the distinction between apps which fall under the regulatory framework of medical devices and other apps is unclear, given that health and wellbeing apps out of the scope of the medical devices framework are not subject to the same safety controls and those apps in the "grey zone" may pose risks similar to those of medical devices. Several replies also indicated that safety risks can originate from non-embedded software and apps that do not respect data protection principles by accessing or collecting sensitive data without informing the user or requesting consent for processing these personal data.

Source: <https://ec.europa.eu/digital-single-market/en/news/synopsis-report-public-consultation-safety-apps-and-other-non-embedded-software>; Guidelines on the qualification and classification of stand-alone software used in healthcare within the regulatory framework of medical devices, MEDDEV 2.1/6 January 2012

RECONCILING RISKS AND BENEFITS OF DATA USE: EXAMPLES OF RECENT POLICY ACTIONS

Today huge amounts of personal data can be collected, transferred and stored by mHealth tools. Some of the data collected may be volunteered or knowingly and willingly provided by the individual. But an increasing share of the data will be observed. MHealth apps, in particular, rely on accessing a broad range of personal data to work properly. The massive flow and storage of data can increase the potential of data theft or misuse by malicious actors and other consequences of a data security breach, the risks of which, as noted previously, may not be easy to ascertain. New and powerful data analytics tools also make it increasingly easy to infer information about individuals, even if they never shared this information.

Appropriate reconciliation of the risks and benefits associated with health data use in the mHealth ecosystem is therefore necessary if the interests of both individuals and societies are to be best served. This requires transparency, an understanding of the reasonable expectations of individuals, and the development of a shared view of how best to serve the public interest in both the protection of health data privacy and in the benefits to individuals and to societies from health data availability and use. The breadth and scale of data collection practices for mHealth is giving rise to new challenges in the implementation of existing data protection standards and procedures that need to be addressed, such as consent to personal data collection and use. There is therefore growing need for consensus on the framework conditions within which mHealth data and related apps can be appropriately governed to enable or support the delivery of high quality health care with consideration of the dignity of all patients.

The OECD Recommendation on Health Data Governance

As mentioned in the introduction, one recent effort to advance policies in this domain is the OECD Recommendation on Health Data Governance. In January 2017, OECD Health Ministers welcomed the Recommendation. The Recommendation sets out twelve principles (Table 1) which aim to provide guidance to governments on the framework conditions that can encourage greater availability and processing of health data within countries and across borders for health-related public policy objectives, while ensuring that risks to privacy and security are minimized and appropriately managed.

Table 1. OECD Draft Council Recommendation on Health Data Governance - Key Principles

Engagement and participation	Approval procedures for the use of personal health data
Coordination and cooperation	Public disclosure and transparency
Capacity of public sector health data systems	Recognition of the role of technology
Clear provision of information	Monitoring and evaluation mechanisms
Effective consent and choice mechanisms	Training and skills development in privacy and security
Controls and safeguards	Certification or accreditation

Source: E. Ronchi, OECD-Harvard Global Health Institute Workshop (2016)

The Recommendation sets the conditions for greater harmonization so that more countries are able to benefit from statistical and research uses of data in which there is a public interest, and from international comparisons.

Enhancing Patient Access to and Control over their Data

Individual countries have also taken related steps through a set of efforts focused on enhancing patient access to and control over their data. Examples include:

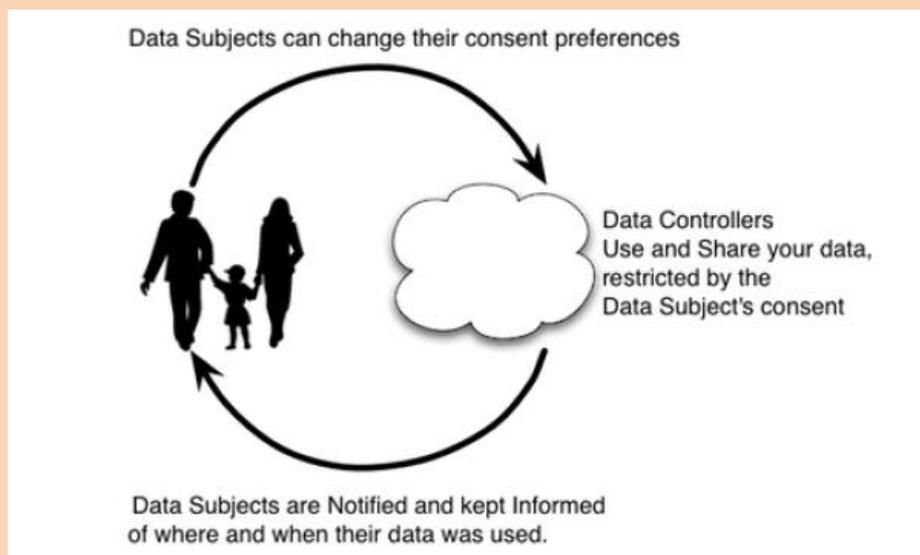
New Consent Models

An important requirement prior to any personal data collection is the issue of obtaining patient consent. The requirement for consent is underpinned by ethical principles of respect for persons and individual autonomy. Consent is also the basis for data protection and privacy law in most countries. Within the medical/scientific field, informed consent generally presumes the ability to indicate clearly to the participant the use and purpose of the particular research activity. Within the digital environment, data is a resource that can be used and reused, often in ways that were inconceivable at the time the data was collected. It is thus possible to learn about individuals far more than most people may anticipate at the point of data collection. Traditional approaches to informed consent are questionable in this environment. And anonymity can no longer be guaranteed. Even if every individual piece of information is stripped of personal information, in a big data environment as noted in the introduction, the risk of re-identification is very high, particularly when data sets are linked⁶. These challenges are compounded by limitations on traditional technologies used to protect privacy (such as de-identification). New approaches are clearly needed to meet ethical and legal requirements for consent and to accommodate the changes in data use, medical and research practices. Approaches recently proposed include “adaptive” or “dynamic” models of consent, whereby (following the initial “general” consent) participants would be asked to re-consent for any “new” direction

⁶ <https://www.itnews.com.au/news/health-pulls-medicare-dataset-after-breach-of-doctor-details-438463>

of travel/use of their data, potentially using web-based communication tools. This approach is ‘dynamic’ because it allows interactions over time; it enables participants to consent to new projects or to alter their consent choices in real time as their circumstances change and to have confidence that these changed choices will take effect (Kaye, 2014).²²

Figure 3. Dynamic Consent



Source: E. Vayena OECD-Harvard Global Health Institute Workshop (2016)

Right to Data Portability

Another response has been to consider the question of whether an individual should have the right to receive the personal data concerning him or her, which he or she has provided to a data controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided. This right has been called ‘data portability’. The EU’s new data protection regulation – the GDPR – sets out a ‘right to data portability’ in Article 20. This Article provides that individuals shall have the right to receive the personal data that they have ‘provided to’ a data controller ‘in a structured, commonly used and machine-readable format’ and the right to transfer that personal data from one controller to another without hindrance. Furthermore, where it is technically feasible, the individual has the right to have the personal data transferred directly from one controller to another. In Europe, there is ongoing debate about the practical challenges of implementation of such a right and the pros and cons of doing so. There has also been discussion of whether such a right would be best implemented through privacy, consumer protection or competition law.

Enhancing Individuals’ Access to their Own Data.

Other examples of initiatives aiming at enhancing individuals’ access to data include the UK ‘Midata’ (then ‘mydata’) and the US “My Data” initiatives. Launched in the UK in 2011, Midata seeks to give consumers access to the electronic information that companies hold about their transactions in a machine-readable and portable format- It focuses on three sectors: energy supply; the mobile phone sector; and the financial sector (accounts and credit cards). The US ‘My Data’ programme similarly includes a number of initiatives that facilitate access by consumers to

their own personal data in particular sectors. An example is the 'Blue Button' initiative which is a hybrid initiative (applicable to public and private sector healthcare providers) that seeks to expand patients' access to their medical records.

New Health Data Cooperatives

Another wave of new initiatives to empower citizens is based on the concepts of individual data donation within data cooperatives that provide platforms to safely store, manage and share personal health-related data. Such health data platforms or cooperatives are solely owned and controlled by their members and not by shareholders. Members determine which data they want to share for example with doctors or to contribute to research for the benefit of their health and that of society. Members also decide how the revenues generated by granting third parties access to the anonymized data that they agreed to share, should be invested in research, information or education.

PRIORITY AREAS FOR FUTURE COLLABORATIVE EFFORTS ACTIONS

The workshop, co-organised with the Harvard Global Health Institute, was also an opportunity to discuss and determine where the OECD can provide further policy insight and expertise. There is today a window of opportunity for cross-country collaboration and learning to advance evidence-based mHealth policies. In particular experts voiced support for international action in three areas where the OECD may decide to do follow-on work summarized below.

Support an Agenda for Evidence-based Implementation of MHealth

The conference revealed that many countries are struggling with the same mHealth-related policy challenges. An area of common interest is the development of a common conceptual framework that can help consolidate the many existing pilot initiatives, guide evaluation, and assist implementation. The WHO is currently in the process of conducting a systematic review of evidence on mHealth in specific sectors of application and could extend this review and validate its methodology in a few OECD countries. Another approach could be to identify core indicators to review countries' "policy readiness" against the OECD Recommendation on health data governance and the WHO eHealth policy frameworks specifically to ensure that foundational/enabling policy frameworks are in place and can support mHealth and other eHealth policy efforts.

Support the Development of Internationally-agreed Quality Assurance Criteria for Health and Wellness Apps

In the area of quality assurance, public and private stakeholders continue to strive to find ways to address concerns on the safety, privacy, security, effectiveness, and performance associated with the use of health and wellness apps. A first potential set of actions could center on reviewing current quality assurance approaches across public and private sectors, identifying good practice in addressing data governance-related risks, ensuring robust digital risk management and compliance with medical evidence base. The objective would be to set out a roadmap for international co-operation in developing common high-level criteria and guidance for the evaluation, adoption and use of health and wellness apps that are not considered medical devices and are therefore not subject to specific evaluation. In this process, the role of private sector players, particularly multinational companies who host major app stores, should be explored. For example, Apple has taken steps to try to improve the safety and effectiveness of health and wellness apps. These efforts complement and could work in concert with policy efforts of OECD countries.

Examine the Opportunities and Challenges in Enhancing Users' Access and Control over their Data

While there is generally good agreement on the potential benefits of enhanced consumer/user control over their health and wellness data, the attainment of this goal pose policy challenges. There is an evidence gap in this area and additional policy work to examine opportunities and challenges is needed. Various rationales are for example, advanced to support new forms of consent, and data portability. On the latter, a common starting place is the notion that data portability can empower individuals as well as lead to greater growth and welfare benefits. However, data security is perhaps the most significant impediment to data portability initiatives, as verification of identification continues to be a challenge for content and service providers. A second major challenge for these

initiatives relates to interoperability. If the right to data portability requires companies to adjust their technical capacity to provide access to data in an accessible and interoperable format this will also increase business costs. At present, the business plans of many digital providers are based in part on the expectation that they will not need to share or transfer their customer data, in particular with competitors. A third concern is that data portability might have negative implications for equality and diversity- as not all users have the required digital literacy. Although savvy consumer might take advantage of data portability opportunities, less skilled and privacy savvy consumers are not likely to do so.

These areas represent substantive and important work that would fuel cross-country efforts – both among and beyond OECD countries - to collaborate in advancing evidence-based mHealth policies. Pursuing this work is critically important to ensure that existing and future mHealth applications lead to better health in an environment that fosters trust.

REFERENCES

1. OECD-Harvard Global Health Institute 2016 Workshop: Mobile technology-based services for global health and wellness: Opportunities and challenges. <http://www.oecd.org/sti/ieconomy/mobile-technology-based-services-for-global-health.htm> Accessed Nov. 23, 2017.
2. World Health Organization. World Report on Ageing and Health.; 2015. www.who.int/. Accessed May 24, 2017. ; R. Osborn, D. Moulds, D. Squires, M. M. Doty, and C. Anderson, "International Survey of Older Adults Finds Shortcomings in Access, Coordination, and Patient-Centered Care," Health Affairs Web First, published online Nov. 19, 2014.
3. research2guidance. mHealth App Developer Economics 2014.; 2014. <https://research2guidance.com/product/mhealth-app-developer-economics-2014/> Accessed Nov. 24, 2017.
4. Diane Doebele Koch JR. Is the HIPAA Security Rule Enough to Protect Electronic Personal Health Information (PHI) in the Cyber Age? *J Health Care Finance.* 2016;43(3). <http://healthfinancejournal.com/index.php/johcf/article/view/67> Accessed Nov. 24, 2017.
5. De Montjoye Y-A, Hidalgo CA, Verleysen M, Blondel VD. Unique in the Crowd: The privacy bounds of human mobility. *Sci Rep.* 2013;3(1):1376. doi:10.1038/srep01376.
6. Wesolowski A, Buckee CO, Bengtsson L, Wetter E, Lu X, Tatem AJ. Commentary: Containing the Ebola Outbreak - the Potential and Challenge of Mobile Network Data. *PLoS Curr.* 2014. doi:10.1371/currents.outbreaks.0177e7fcf52217b8b634376e2f3efc5e.
7. Lee Y, Chang H. Ubiquitous health in Korea: progress, barriers, and prospects. *Healthc Inform Res.* 2012;18(4):242-251. doi:10.4258/hir.2012.18.4.242.
8. United Nations. The Millennium Development Goals Report 2015.; 2015. [http://www.un.org/millenniumgoals/2015_MDG_Report/pdf/MDG 2015 rev \(July 1\).pdf](http://www.un.org/millenniumgoals/2015_MDG_Report/pdf/MDG%2015%20rev%20(July%201).pdf) Accessed Nov. 24, 2017.
9. Pérez-Lu JE, Iguñiz Romero R, Bayer AM, García PJ. Reduciendo las inequidades en salud y mejorando la salud materna mediante la mejora de los sistemas de información en salud: Wawared Perú. *Rev Peru Med Exp Salud Publica.* 2015;373-377. <http://pesquisa.bvsalud.org/bvsvs/resource/es/lil-753275> Accessed Nov. 24, 2017.
10. Mukund Bahadur K-C, Murray PJ. Cell phone short messaging service (SMS) for HIV/AIDS in South Africa: a literature review. *Stud Health Technol Inform.* 2010;160(Pt 1):530-534. <http://www.ncbi.nlm.nih.gov/pubmed/20841743> Accessed Nov. 24, 2017.
11. Lester RT, Ritvo P, Mills EJ, et al. Effects of a mobile phone short message service on antiretroviral treatment adherence in Kenya (WelTel Kenya1): a randomised trial. *Lancet.* 2010;376(9755):1838-1845. doi:10.1016/S0140-6736(10)61997-6.
12. Pop-Eleches C, Thirumurthy H, Habyarimana JP, et al. Mobile phone technologies improve adherence to antiretroviral treatment in a resource-limited setting: a randomized controlled trial of text message reminders. *AIDS.* 2011;25(6):825-834. doi:10.1097/QAD.0b013e32834380c1.
13. ITU. ICT Facts and Figures.; 2016. <http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf> Accessed Nov. 24, 2017.

14. Welz T, Herbst K. Anonymous HIV Testing With Participant-Controlled Access to Results Using Handheld Computers: A New Model of HIV Testing Used in a Household Survey in Rural South Africa. *Sex Transm Dis*. 2008;35(4):372-376. doi:10.1097/OLQ.0b013e31815fd3fc.
15. WHO | Launch of mHealth toolkit to help innovators scale up projects for reproductive, maternal, newborn, child and adolescent health. WHO. 2016. <http://who.int/reproductivehealth/topics/mhealth/maps-toolkit/en/> Accessed Nov. 24, 2017.
16. ITU. National eHealth Strategy Toolkit.; 2012. http://www.itu.int/pub/D-STR-E_HEALTH.05-2012 Accessed Nov. 24, 2017.
17. Comstock J. Survey: 32 Percent of Mobile Device Owners Use Fitness Apps | MobiHealthNews. <http://www.mobihealthnews.com/29358/survey-32-percent-of-mobile-device-owners-use-fitness-apps> Accessed Nov. 24, 2017.
18. Singh K, Drouin K, Newmark LP, et al. Developing a Framework for Evaluating the Patient Engagement, Quality, and Safety of Mobile Health Applications. <http://www.commonwealthfund.org/publications/issue-briefs/2016/feb/evaluating-mobile-health-apps> Accessed Nov. 24, 2017.
19. NHS UK. Digital Apps Library. <https://apps.beta.nhs.uk/> Accessed Nov. 24, 2017.
20. My Health Apps. <http://myhealthapps.net/about> Accessed Nov. 24, 2017.
21. Huckvale K, Car J, Tilney M, Benghozi P-J, Car J. Unaddressed privacy risks in accredited health and wellness apps: a cross-sectional systematic assessment. *JAMA*. 2014;311(14):1447. doi:10.1001/jama.2014.1106.
22. Kaye J, Whitley EA, Lund D, Morrison M, Teare H, Melham K. Dynamic consent: a patient interface for twenty-first century research networks. *Eur J Hum Genet*. 2015;23(2):141-146. doi:10.1038/ejhg.2014.71.