Task Force 4
Digital Transformation

Policy brief

OPPORTUNITIES FOR INTERNATIONAL COOPERATION ON DIGITAL HEALTH. LESSONS FROM THE EUROPEAN UNION

SEPTEMBER 2021

Nadina Iacob Centre for European Policy Studies (CEPS)
Felice Simonelli Centre for European Policy Studies (CEPS)

T20 NATIONAL COORDINATOR AND CHAIR
ISPI

T20 CO-CHAIR
IAI

T20 SUMMIT CO-CHAIR
Università Bocconi MILANO

THINK20 ITALY 2021

G20 ITALIA 2021

ABSTRACT

The COVID-19 pandemic has brought to the forefront the role of sharing quality data in a timely manner to inform crisis management, public health and research. Moreover, the value of data is enhanced when countries cooperate and facilitate cross-border data flows. Policymakers should harness the value of health data and engage in a global discussion that strives for common, cross-border and effective digital health solutions to improve health outcomes for all. This policy brief argues for action in three key areas: establishing technical and legal building blocks, gaining end users' trust, and fostering research, innovation and competition.

CHALLENGE

Digital health plays a pivotal role in supporting the **achievement of the Sustainable Development Goals (SDGs)**, especially SDG 3, which aims to "ensure healthy lives and promote well-being for all at all ages" (Asi and Williams 2018; Novillo-Ortiz, Marin and Saigi-Rubio 2018). Bolstered by technological developments, **the digital healthcare sector is expected to grow rapidly** around the world, with an estimated sixfold increase in market size between 2019 and 2026 that is set to reach almost US$ 640 billion (Gupta 2021). The COVID-19 pandemic is certainly contributing to this trend. Telemedicine, for instance, has become one of the tools for bridging the gap in the safe provision of medical services during the pandemic (Vidal-Alaball 2020), and emerging legislation in some countries is likely to support its use beyond the pandemic (see, for instance, Matthies, 2021). As digital health applications expand, **ensuring the proper governance of digital health ecosystems** is becoming a key priority, for both national policymaking and international cooperation.

A **digital health ecosystem** includes stakeholders, technologies, data infrastructure and governance frameworks enabling digital health solutions. As the digital transformation permeates everyday life, real-world data[1] increasingly abound (including data generated by users of mobile and wireless devices) and generate more opportunities for innovative, **data-based healthcare services and therapies**. This also paves the way for the secondary use of health data that goes beyond the direct delivery of healthcare services and enables wider applications such as **research, quality and/or safety measurement, public health, policymaking, and development of private services** (Safran et al. 2007).

The COVID-19 pandemic has brought to the forefront the role of data in crisis management, public health and research, emphasising that sharing quality data in a timely manner is crucial at different stages of decision-making, research, and healthcare service provision. At the onset of the pandemic, heterogeneous data and inadequate data sharing created hurdles for policymakers and researchers alike. In the case of the EU, even in the framework of the historical cooperation between the bloc's Member States, the lack of consistent data jeopardised the joint response to the crisis (Renda and Castro 2020). International research efforts were also hindered by, for example, incompatible data formats, partial data reporting that limited data comparability, and lack of standardised processes for data sharing (LoTempio et al. 2020).

One of the key messages from this experience is **that the value of data is enhanced when countries cooperate and facilitate cross-border data flows**. To face the health challenges of the future, it is time to tap into the momentum for change. The use of health data goes well beyond COVID-19 itself. Quality data and emerging technologies are opening up the way for a transnational digital health ecosystem to blossom. Such an ecosystem, however, faces **major challenges**, from interoperability of data and processes to standardisation, data quality to liability in the digital age, competition issues to data protection, and digital and data literacy to user trust.

PROPOSAL

At this point, as emphasised by the World Health Organisation's Global Strategy on Digital Health (WHO 2020), **setting the tone for strategic decisions and cooperation** is vital. And the G20 can and should stay ahead of the game to harness the potential of digital health. It is crucial not to be caught off guard by technologies moving faster than the policy process. For a **well-functioning and transnational digital health ecosystem**, that strives towards common, cross-border and effective digital health solutions to **improve health outcomes for all**, the global discussion needs to start now. In this context, policymakers should focus on establishing technical and legal building blocks, gaining end users' trust, and fostering research, innovation and competition. These key steps could facilitate data sharing for **better health outcomes** and enable **research and novel data-driven solutions for healthcare and well-being**. Any new measure must, however, be part of a wider rule-based framework governing cross-border data flows between countries and **ensuring privacy and security**.[2]

COOPERATING FOR COMMON BUILDING BLOCKS

In a well-functioning ecosystem, data would flow in a standardised manner[3] between different systems against a clear framework of rules for data sharing (including data protection, privacy, liability, and cybersecurity) through the safe interactions of all stakeholders. Public authorities are, therefore, called to set rules that are fit for purpose, promote standardisation, and ensure **legal and technical harmonisation beyond national borders**.

Harmonising rules for health data protection. The EU General Data Protection Regulation (GDPR) plays a central role in fostering trust and introducing a level playing field for data protection across Europe. It is a vivid example of how strict data protection rules are compatible with and can even foster innovation and the cross-country provision of data-based services.[4] For businesses seeking to operate cross-border – particularly small and medium-sized enterprises (SMEs) – fragmented rules are worse than loose rules, as fragmentation creates hurdles and translates into compliance burdens. To create a well-functioning digital health ecosystem that goes beyond national borders, the G20 can play a coordinating role, monitoring how relevant rules evolve and, to the extent that is possible, promoting the introduction of health data protection rules that are both stringent (to increase end user trust) and cohere with the development of transnational digital health ecosystems (facilitating data exchange and the provision of data-based services across countries under necessary safeguards for privacy and security).

Fostering cooperation for living and dynamic standards. Technical solutions enabling data exchanges are the backbone of effective health data sharing. Cooperation is essential to ensure the uptake of standards and technical specifications. At EU level, by way of example, recommendations on a European electronic health record exchange format were recently introduced (Commission Recommendation C(2019)800). More widely, continued

cooperation concerning standards in the field of digital health should be promoted. As the field is continuously evolving, agreeing on a certain set of standards at a given point in time will likely not be sufficient. The solution will rather be a "living and dynamic standard", or "living dictionary", that would also capture the liveliness of the field; new terms and developments should be incorporated, and outdated ones should be discarded in a flexible and rapid manner to keep up with innovation in the field.

Updating existing liability rules. With the proliferation of new digital technologies and services, current liability frameworks are put to the test (the EU one, for example, is based on the Product Liability Directive that dates back to 1985: Council Directive 85/374/EEC). Existing liability rules should be carefully revised to take into consideration the challenges posed by the digital era (Yang and Silverman 2014; Terry and Wiley 2016; Price et al. 2019; Expert Group on Liability and New Technologies, 2019), especially when it comes to extra-contractual liability as well as services and applications based on health data that do not fall directly under the scope of sector-specific legislation (such as the EU Medical Device Regulation that sets rules for products and equipment intended for medical use; Regulation (EU) 2017/745). As new applications such as wearable devices, telemedicine, and AI-based applications impact the provision of healthcare and wellbeing services, it is important to clearly define the roles and responsibilities of key stakeholders, such as patients, medical doctors, hardware producers, software developers, data providers and digital marketplace owners (Parimbelli et al. 2018). This is key to increasing legal certainty, reducing litigation costs, instilling trust in the system and, ultimately, convincing more stakeholders to participate.

GAINING PUBLIC TRUST

Recent controversies, such as Google's acquisition of Fitbit, prompted warnings of potential detrimental effects on consumers (BEUC, 2020), and privacy concerns related to digital solutions aimed at containing the coronavirus (Renda, 2020) have shown that **gaining and maintaining public trust** is crucial. A digital health ecosystem should gain the trust of end users and encourage health data sharing.

Increasing accountability and transparency. To gain end users' trust, it is important to mitigate their concerns about what happens to their data, who has access to them, how they are protected, who is responsible for data privacy breaches and who one can appeal to in case problems arise. Businesses wishing to engage in health data sharing should be prepared to provide clear and concise answers to such questions from their users. In this regard, accountability mechanisms for stakeholders sharing and using health data should consist of internal control systems that produce evidence such as audit reports, which can be presented not only to users but also to supervisory bodies. For effective communication, the information provided to users should be as clear and concise as possible, giving straight answers to questions rather than overloading them with information.

Creating a "privacy label". To increase transparency and address potential concerns around data privacy and security, a "privacy label" for health apps could be established. Such a label should contain information about the underlying technology and the level of privacy of the application in a clear and distilled fashion, in the same way as nutrition labels. Privacy labels could either be introduced by public authorities as a requirement for health apps being allowed on the market, or they could be a self-regulatory measure implemented independently by app developers, allowing service providers to distinguish themselves by the importance they place on the security and privacy of the user's data.[5]

Developing clear and transparent rules for data access. The sensitivity of health data requires serious reflection on data access rights for different categories of stakeholders, accounting for their ability to protect and properly handle such data. Data access should allow the development of innovative data-based services within a framework that fosters trust and cooperation. As such, access to specific types of health data for service providers could be made contingent on prior authorisation by public authorities.

Improving data quality. Multiple stakeholders have a role to play in ensuring the quality of the data shared in a digital health ecosystem. Low-quality data may lead to services of equally poor quality. For the proper functioning of digital health ecosystems, a legal framework helping identify who is liable for the quality of data shared and used must be established. Such a framework would most likely need to acknowledge the chain of responsibility when data are shared: the data providers would be responsible for the data they collect and make available, the providers of data-based services would be responsible for any issues resulting from their processing of such data, while intermediaries would be responsible for the general governance of data marketplaces and exchange platforms. The goal of such a framework should be to establish clear rules on liability where health data is of low quality. This would reduce uncertainty for businesses and litigation costs, provide incentives to improve data quality, and ultimately increase user trust.

Equipping patients and professionals with the right set of skills. Full trust cannot be achieved without sufficient knowledge. There is an urgent need to educate end users (consumers and patients) and health professionals so that they can effectively use and benefit from new data-driven solutions for healthcare (European Health Parliament, 2016). Targeted training for healthcare professionals and information campaigns to raise awareness among individuals (made available, for instance, by public authorities in a format that is easy to understand) can help bridge the gap in digital and data literacy and facilitate the uptake of innovative digital health solutions.

SPURRING RESEARCH, INNOVATION, AND COMPETITION

Digital health is still in its infancy. When creating a digital health ecosystem, the mistakes made in other digital ecosystems (where market concentration is incredibly high and a few large players own, use, and provide data on a global scale) should be rigorously avoided. **Competition, research, and innovation should be continually fostered** to improve the quality of digital health services and, ultimately, health outcomes.

Enhancing interoperability. The increasing amount of health data generated by a variety of sources holds great potential for a digital health ecosystem. Nevertheless, limited interoperability resulting from the deliberate decision of some market players to follow their own specifications for their services may lead to important lock-in effects. A host of areas within digital health can be significantly enhanced with more interoperable data. For instance, interoperable data can enhance international cooperation and the coordinated response to global threats such as the COVID-19 pandemic. Promoting the use of common standards and specifications is essential for unlocking the potential of health data, and for ensuring that data are not confined to silos and that a competitive market allowing for data sharing and reuse is in place.

Enabling data portability. In the EU, the right to data portability,[6] enshrined in the EU GDPR (GDPR, Regulation (EU) 2016/679), has created an opportunity for more user-centric and user-driven data sharing. Such a right should be granted by all countries aiming to create a dynamic digital health ecosystem. The right of the user to receive their data, however, does not necessarily mean that the data can be easily reused for other services. Legal provisions supporting data portability should always be complemented with technical provisions specifying the technical means through which access to data is granted. For instance, an application programming interface (API)[7] could be the technical tool to enable easier access to data by new service providers.

Ensuring fair access to health data. Accessing health data may be too expensive for some categories of stakeholders, such as academic and research organisations or SMEs. To support research and innovation and encourage competition through the presence of SMEs in the market, it is important to introduce price-discrimination schemes for health data that grant fair access to specific categories of stakeholders.

Developing a framework for the secondary use of health data. Legal uncertainty and fragmentation due to diverging national rules are impinging on the secondary use of health data. A case in point is the EU GDPR, which creates impediments to data sharing with researchers outside the EU (Allea, EASAC and FEAM, 2021). Enabling the secondary use of health data while also ensuring a high level of data protection and privacy is crucial for building a well-functioning digital health ecosystem. Research could benefit from a framework facilitating the sharing of health data across borders, thus enabling the creation of a larger pool of data that can then be used to carry out studies. With the rise of big data, opportunities in this field can be significant, but without clear rules risks can also proliferate. The Finnish national law on the secondary use of health and social data[8] is an example of policy action supporting legitimate developments in this field. The G20 should foster cooperation on the governance of the secondary use of health data that can bolster research and innovative data-based applications on a global scale.

NOTES

[1] Real-world data are generally defined as data gathered outside the context of randomised controlled trials. Real-world data can include, for instance, electronic health records, registries, administrative data, health surveys, and data from mobile apps (Garrison et al, 2007).

[2] Establishing a rule-based framework for cross-border data flows is a necessary action, especially if one considers the ever more central role that data is playing in the economy and society in general. Nevertheless, achieving such a framework is not without challenges. The recent case of the invalidation of the Privacy Shield (which provided the framework for lawful personal data transfers from the EU to the US based on data protection requirements and safeguards up to July 2020) shows the difficulties in establishing rules for cross-border data exchanges between different national legal frameworks (Mildebrath 2020). Cooperation is nevertheless possible, as evidenced, for instance, by the 2019 EU-Japan adequacy agreement for safe data flows. For further details please see: European Commission (2019), European Commission adopts adequacy decision on Japan, creating the world's largest area of safe data flows (https://ec.europa.eu/commission/presscorner/detail/en/IP_19_421).

[3] Standardisation is one of the central elements to support the development of digital health, ensuring the comparability of data (for instance for research purposes) and reducing redundancies. Nevertheless, the adoption of common standards is impacted by specific challenges faced by countries, including the need for funding for the development and implementation of standards, the need for appropriate legal frameworks, as well as the need for engaging as many countries as possible in the process of developing standards. International cooperation and support through international fora like the World Health Organisation could help mitigate against these challenges. For further details please see: World Health Organisation (2012), WHO Forum on Health Data Standardisation and Interoperability, (https://www.who.int/ehealth/WHO_Forum_on_HDSI_Report.pdf).

[4] Please note, however, that some differences within the EU can still arise because of the way in which the GDPR is applied at national level. This is especially true in the health sector, as health data are considered 'sensitive', and this allows member states to introduce more stringent provisions as they deem necessary.

[5] The level of data privacy ensured by the app could be vetted through a set of questions related to how the data are stored and processed. The adoption of such a label could be based on an international standard on healthcare and wellness apps that is currently being developed by two standards organisations: ISO and CEN. The draft standard, ISO TS 82304-2 "Health software – Quality and reliability of health and wellness apps", assess apps on multiple levels, including the security of data. CEN/TC 251 Health Informatics (2021), Draft standard on health wellness apps open for comments, (https://www.ehealth-standards.eu/2021/03/08/draft-standard-on-health-wellness-apps-open-for-comments/).

[6] In a nutshell, users of digital services have the right to: i) receive their personal data from the service provider in a structured, commonly used, and machine-readable format; ii) transmit those data to another service provider; and iii) have their personal data transmitted directly from one service provider to another, where technically feasible.

[7] APIs are a technical solution that support the interoperability of a given system or application by providing an interface through which other systems and applications can link, facilitating data exchanges (Article 29 Working Party 2016).

[8] For further details, please see "Secondary use of health and social data" (Ministry of Social Affairs and Health, Finland) (https://stm.fi/en/secondary-use-of-health-and-social-data).

REFERENCES

Allea, EASAC and FEAM, *International Sharing of Personal Health Data for Research*, 2021 https://easac.eu/fileadmin/PDF_s/reports_statements/Health_Data/International_Health_Data_Transfer_2021_web.pdf

Article 29 Working Party, Guidelines on the right to data portability, 2016, p. 5 https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf

Asi Y.M. and C. Williams, "The role of digital health in making progress toward Sustainable Development Goal (SDG) 3 in conflict-affected populations", *International Journal of Medical Informatics*, vol. 114, 2018, pp. 114-20

BEUC, Google-Fitbit merger - Competition concerns and harms to consumers, 2020 www.beuc.eu/publications/google-fitbit-merger-competition-concerns-and-harms-consumers/html

CEN/TC 251 Health Informatics, Draft standard on health wellness apps open for comments, 2021 https://www.ehealth-standards.eu/2021/03/08/draft-standard-on-health-wellness-apps-open-for-comments/

Commission Recommendation on a European Electronic Health Record exchange format (C(2019)800), 6 February 2019 https://ec.europa.eu/digital-single-market/en/news/recommendation-european-electronic-health-record-exchange-format

Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, OJ L 210, 7.8.1985, pp. 29-33

European Commission, European Commission adopts adequacy decision on Japan, creating the world's largest area of safe data flows, 2019 https://ec.europa.eu/commission/presscorner/detail/en/IP_19_421

European Health Parliament, Committee on Digital Skills for Health Professionals, Digital Skills for Health Professionals, 2016, p. 6 www.healthparliament.eu/wp-content/uploads/2017/09/Digital-skills-for-health-professionals.pdf

Expert Group on Liability and New Technologies, Liability for artificial intelligence and other emerging digital technologies, European Commission, 2019, pp. 27-28 https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDocanddocid=36608

Garrison L.P. Jr., P. J. Neumann, J. Erickson, D. Marshall, and D. Mullins, "Using Real-World Data for Coverage and Payment Decisions: The ISPOR Real-World Data Task Force Report", *Value in Health*, vol 10, no. 5, pp. 326-35

Gupta D., "How Mobile Apps Are Transforming the Healthcare Industry?", Appinventiv Blog, 31 March 2021 https://appinventiv.com/blog/mobile-apps-transforming-healthcare-industry/

LoTempio J., S. D'Andre, R. Yarvitz, A.D. Vilain, E. Vilain, and E. Délot, "We Can Do Better: Lessons Learned on Data Sharing in COVID-19 Pandemic Can Inform Future Outbreak Preparedness and Response", *Science and Diplomacy*, vol. 9, no. 2, 2020

Matthies H., "Here to stay: Digital health in times of COVID-19 – a German deep dive", in Health Innovation Hub Magazin, 2021 https://hih-2025.de/here-to-stay-digital-health-in-times-of-COVID-19-a-german-deep-dive/

Mildebrath H., "The CJEU judgment in the Schrems II case", European Parliamentary Research Service, 2020 https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf

Novillo-Ortiz D., H. De Fátima Marin, and F. Saigí-Rubió, "The role of digital health in supporting the achievement of the Sustainable Development Goals (SDGs)", *International Journal of Medical Informatics*, vol. 114, 2018, pp. 106-07

Parimbelli E., B. Bottalico, E. Losiouk, M. Tomasi, A. Santosuosso, G. Lanzola, S. Quaglini, and R. Bellazzi, "Trusting telemedicine: A discussion on risks, safety, legal implications and liability of involved stakeholders", *International Journal of Medical Informatics*, vol. 112, 2018, pp. 90-98

Price W. Nicholson II, S. Gerke, and I. Glenn Cohen, Potential Liability for Physicians Using Artificial Intelligence, *JAMA*, October 4, 2019

Renda A., "Will privacy be one of the victims of COVID-19?", CEPS In Brief, 2020 www.ceps.eu/will-privacy-be-one-of-the-victims-of-COVID-19/

Renda A. and R. Castro, "Towards Stronger EU Governance of Health Threats after the COVID-19 Pandemic", *European Journal of Risk Regulation,* 11, no. 2, 2020, pp. 273-82

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) (Text with EEA relevance) OJ L 119, 4.5.2016, pp. 1-88

Safran C., M. Bloomrosen, W.E. Hammond, S. Labkoff, S. Markel-Fox, P.C. Tang, and D.E. Detmer, "Toward a National Framework for the Secondary Use of Health Data: An American Medical Informatics Association White Paper", *Journal of the American Medical Informatics Association*, vol. 14, issue 1, 2007, pp. 1-9

Terry N.P. and L.F. Wiley, Liability for Mobile Health and Wearable Technologies, *Annals of Health Law*, vol. 25, 2016, pp. 62-97

Vidal-Alaball J., R. Acosta-Roja, N. Pastor Hernández, U. Sanchez Luque, D. Morrison, S. Narejos Pérez, J. Perez-Llano, A.S. Vèrges, and F. López Seguí, "Telemedicine in the face of the COVID-19 pandemic", *Atención Primaria*, vol. 52, issue 6, 2020, pp. 418-422

World Health Organisation, WHO Forum on Health Data Standardisation and Interoperability, 2012 https://www.who.int/ehealth/WHO_Forum_on_HDSI_Report.pdf

World Health Organization, *WHO Guideline: Recommendations on digital interventions for health system strengthening*, 2019, p. 91 https://apps.who.int/iris/bitstream/handle/10665/311941/9789241550505-eng.pdf

World Health Organization, *Global strategy on digital health 2020-2025*, 2020 www.who.int/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc-79ca799dce4d.pdf

Yang Y.T. and R.D. Silverman, "Mobile Health Applications: The Patchwork Of Legal And Liability Issues Suggests Strategies To Improve Oversight", *Health Affairs*, vol. 33, no. 2, 2014

ABOUT THE AUTHORS

Nadina Iacob Centre for European Policy Studies (CEPS), Brussels (Belgium)

Research Fellow at CEPS. Her research interests lie in the potential of the digital transformation and its implications across a variety of policy areas. Her recent work focuses on the emerging governance architecture for digitalisation and data sharing in areas including healthcare and the public sector.

Felice Simonelli Centre for European Policy Studies (CEPS), Brussels (Belgium)

Associate Senior Research Fellow at CEPS. His research activities focus on better regulation, digital economy, industrial competitiveness, research and innovation, energy and energy-intensive industries.