Health and Care in the Digital Single Market

Reflection paper

September 2017

european public health alliance

Health and Care in the Digital Single Market

Reflection paper

1 Policy context

This report follows up on previous EPHA policy documents and articles on the topic of health data and personal data protection, taking into account the developments at European (EU) and national levels in the area of digital health

Over recent years, the General Data Protection Regulation (GDPR) has become one of the most closely followed pieces of EU legislation. It entered into force in May 2016 (and must be transposed into national law by 25 May 2018), replacing Data Protection Directive (95/46/EC) and introduces new obligations on organisations that are processing personal (health) data. While the main aim of the Regulation is to strengthen privacy rights, it also constitutes an important piece of the Digital Single Market Strategy for Europe adopted in 2015[1], an initiative designed to boost digital innovation. In this context, the GDPR seeks to reconcile privacy and innovation by harmonising privacy legislation across the EU.

Data has become an increasingly important topic as a driver of healthcare innovation; however, the path to operationalisation remains unclear in the absence of a common European approach. With more comprehensive and bigger datasets at their disposal, researchers can gain insights into the efficacy of treatments, analyse genetic information and create better connections, and improve prevention by better informing individuals' choices. The data revolution has wide-reaching implications for medicines regulation and care, e.g. self-generated data from mobile applications, wearables and social media, which Europe must continue to discuss with the public health community and end users.

In line with the evolving legislative framework on the protection of personal data, electronic health records (EHR), and the policy debate around Big Data[2], the European Commission is preparing a Communication for release in 2018 that will address the need and scope for further measures in the area of digital health and care. It is expected to emphasise citizen empowerment and patient-centred care and should help to better tackle chronic diseases and to increase understanding of health outcomes. The other key issues will be data sharing to advance research on population health and faster identification of people at-risk of disease, in order to offer preventative interventions or treatment at an earlier stage.

The 'State of Health in the EU' 2017 report recommended the digital transformation of health and care systems as a priority, coupled with patient-centeredness and e-skills development of the health workforce.[3] Taking this further, Council conclusions drafted under the Estonian Presidency in December 2017 note that "new opportunities are arising from big data and improved health analytics capabilities (...)". This translates, *inter alia*, into a call on EU national governments to "improve the

[1] COM(2015) 192 final
[2] See Gesundheit Österreich (2016), *Study of Big Data in Public Health, Telemedicine and Healthcare – Final Report* written for the European Commission. It provides the following definition: "Big Data in Health refers to large routinely or automatically collected datasets, which are electronically captured and stored. It is reusable in the sense of multipurpose data and comprises the fusion and connection of existing databases for the purpose of im-proving health and health system performance. It does not refer to data collected for a specific study."
[3] See https://ec.europa.eu/digital-single-market/en/news/state-health-eu-report-recommends-digital-transformation-health-and-care

comparability, accuracy and reliability of health data" and an invitation to countries and the Commission to "reinforce actions to improve data security". However, a clear vision for the use of Big Data in Europe still appears a long way off.

Personal data plays an invaluable role in health research; to make epidemiological progress, combat rising health inequalities and protect public health. Nevertheless, there is an important balance that needs to be struck between protecting privacy and making the best use of health data.

During 2017, stakeholders were consulted on 'Transformation of Health and Care in the Digital Single Market'[4], in particular on the future of healthcare in a digitised world. EPHA's response emphasises that digital health solutions must be inclusive and ethically integrated into national health systems to ensure improved access to healthcare so that everyone can benefit from the digital revolution See also EPHA's 2014 report on eHealth and health inequalities for the European Commission eHealth Stakeholder Group.[5]

2. The potential of digital health

All organisations processing health data will need to review their existing policies, procedures, and practices to ensure compliance with the GDPR. The Regulation will have an unavoidable impact on hospitals, pharmaceutical companies, academic institutions, and technology companies using health data.

Europe's approach to Big Data is testimony to the importance placed on data as an integral part of health systems, and it is aligned with related European policies (Open Data, Cloud Computing, High-Performance Computing, access to scientific data).

The possibility to analyse ever-larger datasets plays an important role in medical research. Big data could lead to better health outcomes through improved treatment and care. The information held about individuals in their medical records, in medical registries and other databanks provides new opportunities to investigate causes of diseases, the effectiveness of treatments and interventions, and follow up on patients during and after clinical trials. Health data has a value and should be used for medical research under certain conditions and only with appropriate safeguards in place to protect privacy and confidentiality. As health and care are a particularly personal and sensitive domain, health data should never become "commercial" in the sense that they would favour certain people over others. After all, individuals' health and behaviours are linked with their economic, social and cultural environments, which determine health status and strongly influence the choices available to them.

The transition to Big Data and the Internet of Things (IoT) could have a major impact on the healthcare sector, depending on how all the data generated is aggregated, analysed and shared. It could be argued that the healthcare sector is increasingly becoming a massive database collecting information, including clinical, genetic, behavioural and environmental data from various sources and devices including EHRs, genome sequencing, patient registries, social networks and applications that monitor health.

Gathering this wealth of information by tapping into different data repositories and being able to analyse it provides immense potential for improving the effectiveness and quality of healthcare for future generations[3]. Algorithms can already predict disease risk so that it can be prevented or treated at an earlier stage[6]. However, caution must be applied in the use and spread of data: constant

[4] European Commission (2017), Public consultation on Transformation of Health and Care in the Digital Single Market: https://ec.europa.eu/info/consultations/public-consultation-transformation-health-and-care-digital-single-market_en
[5] https://ec.europa.eu/digital-single-market/news/commission-publishes-four-reports-ehealth-stakeholder-group
[6] https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource

monitoring and gathering information from online searches and clicks, social media, mobile transactions, time tracking systems at work and socioeconomic indicators that could be linked with health data can lead to false assumptions. It does not take into account the behavioural aspects of health, personal / family histories and crucial information that healthcare professionals are able to glean during face-to-face consultations. Big Data and IoT might pose major risks to universal access to healthcare, health equity and end users' exclusion from the product development process, leading to "innovations" that may not correspond to real needs nor produce positive health outcomes. The increased role of data in health can be a stressful experience for end users who are unfamiliar with how their data may be used.

One of the supporting tools of the data revolution is cloud computing, a technological development that increases cross-border data management, processing and storage by relying on remote servers. This opens up questions regarding the territorial scope of the EU regulatory framework triggered by the sharing of computing resources rather than relying on local servers or personal devices.[7] When personal data is processed in the cloud, it usually flows through - and is stored in - various countries, which may also be outside the EU. Certain data protection legislation pertaining to providers with no legal entity based in the EU may not provide an equivalent level of protection, which could provide opportunities for exploiting data for commercial and harmful purposes.

Stakeholder perspectives on Big Data are summarised in a recent European Parliament briefing[8]. For example, European Digital Rights (EDRi)[9] is an association of civil and human rights organisations from across Europe that defends rights and freedoms in the digital world. EDRi claims that information technology has a revolutionary impact on our society because it has boosted freedom of communication and democracy. However it has also led to new approaches to surveillance and new technology is increasingly deployed to impose *restrictions* on fundamental rights. A key concern is that Big Data, in combination with other data sources can fundamentally change the very nature of personal data. The European Consumers' Association (BEUC) is concerned that issues of data flows and data localisation between the EU and third countries like the USA should be discussed outside the context of trade negotiations, so as to avoid any weakening of consumers' rights to privacy.[10]

These views are in sharp contrast with industry associations such as Business Europe[11], who believe that a 'free flow of data' initiative is needed to prevent the obligations to store data in a specific country hindering business operations, stating that Europe needs to invest in developing skills such as data analysis. Moreover, DIGITALEUROPE, an association representing the digital technology industry, highlights that Big Data presents enterprises with opportunities to improve their performance, develop new business models and improve products and services. One of their key concerns is that the GDPR introduced new restrictions for Big Data applications[12].

3. Informed consent, informed users?

The first goal of the new EU data protection framework is to increase the scope of data protection laws, require more stringent obligations on anyone handling personal data across the EU and increase the rights afforded to data subjects as regards accessing, modifying and erasing data. Currently, access to one's own personal health data is far from assured in most countries, and some people, e.g. those with specific physical or mental health conditions may not enjoy this right at all.

[7] https://secure.edps.europa.eu/EDPSWEB/edps/lang/en/EDPS/Dataprotection/QA/QA10
[8] Davies, Ron (Sep 2016), Big Data and data analytics. EPRS Briefing. Members' Research Service. PE 589.801
[9] https://edri.org/
[10] BEUC (2017), The challenge of protecting EU consumers in global online markets. http://www.beuc.eu/publications/beuc-x-2017-122_the_challenge_of_protecting_eu_consumers_in_global_online_markets.pdf
[11] https://www.businesseurope.eu/
[12] DIGITALEUROPE (2016), Briefing on Big data and data analytics. The potential for innovation and growth. http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/589801/EPRS_BRI(2016)589801_EN.pdf

Definitions of "personal data" and "sensitive personal data": have both been expanded. The term "genetic data" is introduced, defined as data which includes personal data relating to inherited or acquired genetic characteristics. Although "data concerning health" was protected as a special category under earlier EU data protection legislation, the current GDPR defines it as personal data related to physical or mental health, including the provision of healthcare services. The GDPR now specifically lists genetic data and biometric data as sensitive personal data and permits Member States to introduce further conditions around the processing of these data.

A further major change in the GDPR is that public health institutes and researchers that collect and/or use any data concerning health, genetic or any sensitive personal data must ensure that they adhere to the definition of exceptional circumstances which allow this personal data to be processed. For example, processing is necessary for public interest reasons in the area of public health, such as protection against cross-border health threats (e.g. antimicrobial resistance) or for the purposes of preventive or occupational medicine, medical diagnosis, provision of health or social care or treatment, management of health or social care systems and services, under a contract with a health professional or another person subject to professional secrecy under law ('medical care' grounds).

The GDPR adopts a broad definition of research, encompassing the activities of public and private entities alike. In the age of Big Data, many organisations are involved in data analytics and activities which may be qualified as research. It remains unclear exactly how far the GDPR's research exemption will extend.[13].

EU law on the protection of privacy and personal data enshrines the right to equality and non-discrimination, as well as the right of individuals to receive information about the logic involved in automated decision-making and profiling. Any data processing has to be preceded by pseudonymisation techniques, because the use of non-personal data might impact on individuals' private lives and/or rights and freedoms. Violation of this law could lead to the stigmatisation of whole population groups[14]. Therefore, in the context of health research, the GDPR stipulates that personal data must no longer be ascribed to a specific individual. If an organisation decides to use health data for profiling activities, it must give affected individuals the right to opt out. The only exceptions to the right to opt out are when the subjects originally consented to profiling[15] or where it is necessary for reasons of substantial public interest (e.g. serious threats to cross-border health) and, in both instances, suitable measures to safeguard the individuals' rights and freedoms are implemented.

If an organisation cannot rely on grounds related to medical care, public health, or scientific research, it will have to obtain explicit consent from the individual to process their health data. The requirement under the GDPR for obtaining valid consent is similar to the requirement under the previous Directive. However, the GDPR places the onus on the data controller to demonstrate that consent was given. Therefore, a new designation of consent is provided, defined as a freely given, specific, informed and unambiguous indication, by a statement or clear affirmative action, signifying a person's agreement to the processing of their personal data[16].

With regard to data sharing for public health purposes, the potential of new technology and data for public protection suggests that health and scientific research should be under particular consideration regarding the obligation to gather specific consent from subjects.

Therefore, it is also very important that individuals are accurately informed about their rights and about key concepts such as explicit consent. Consent is at the heart of discussions about data

[13] https://bigdata.fpf.org/wp-content/uploads/2015/12/Tene-Polonetsky-Beyond-IRBs-Ethical-Guidelines-for-Data-Research1pdf
[14] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0044+0+DOC+XML+V0//EN#title1
[15] According to Article 4(4) GDPR, "profiling" refers to (a) automated processing of personal data; and (b) using that personal data to evaluate certain personal aspects relating to a natural person.
[16] https://www.ropesgray.com/newsroom/alerts/2017/02/The-GDPR-Possible-Impact-on-the-Life-Sciences-and-Healthcare-Sectors.aspx

protection and research. Without any doubt, it is an important principle in research and – wherever possible – researchers must seek consent from subjects before using their personal data. However, in some specific instances, it is not possible or impracticable to do so. For example, the additional burden of having to re-contact former participants prior to each new research would render many studies, especially large ones, unworkable in practice and/or prohibitively expensive. It would delay them and increase the time needed to translate results into concrete benefits for individuals and society at large, and to advance disease-specific knowledge. In addition, subjects may not wish to be contacted on several occasions as they perceive this as being uncomfortable, cumbersome or intrusive, which in turn could prompt them to refuse consent. Data subjects could feel trailed by researchers and it could trigger concerns about leaving additional data traces.

4. Outlook

The upcoming Communication from the European Commission, following the public consultation on "Transformation of Health and Care in the Digital Single Market" [17], will provide a first response to the 2017 Council conclusions led by the Estonian Presidency. It should present Europe's vision for the future of healthcare in the digitised world, including the integration of digital health solutions into national health systems in an inclusive and ethical way. It must pave the way for improved access to healthcare and tangible benefits for all.

The Council conclusions on Health in the Digital Society pursue the aim of advancing data-driven innovation in the field of health in Europe, but their main focus is encouraging Member States to "work together to facilitate the necessary convergence in regulatory and governance approaches to the use of health data for research and innovation purposes (...), and, if appropriate, engaging with the bodies responsible for data protection for example in the framework of the European Data Protection Board provided for in the General Data Protection Regulation."[18] They also favour the creation of "decentralised data networks and common platforms" over "unnecessary data storage at a central Union repository".[19]

Data and new technology are continuously gaining in importance and reshaping society, including the health sector. The amount of health data that can be collected and processed is increasing steadily and it would be detrimental to public health if Europe could not take advantage of the new possibilities that Big Data and other developments afford to public health community. The intensification of globalisation, accelerated by the Internet and digital technology, has increased concerns about solidarity and universality – so important in health – in the context of rising healthcare costs and increasing demand.[20] In some parts of Europe, austerity measures introduced stricter eligibility rules and access barriers to health and social care. In such an environment, data sharing could contribute to empowering people as regards their own health and care and to become active proponents of public health measures, by making the benefits felt at a personal level.

The area of digital health is often compared to online banking which, for many people in Europe, has become routine with comparatively few worries about data misuse. The reason why healthcare is trailing behind in terms of digital uptake could well be that it is inherently different from other sectors, involving a greater range of intimate considerations and emotions. Especially since abusing personal health data could lead to increasing health inequalities and marginalisation from the health system. Given the sensitive nature of health data, a key priority must be to prevent any misuse which could

[17] Public consultation on Transformation of Health and Care in the Digital Single Market https://ec.europa.eu/info/consultations/public-consultation-transformation-health-and-care-digital-single-market_en

[18] Council conclusions (2017), op. cit., p.10

[19] Ibid. p.12

[20] Porznold, F. & Kaplan, R.M. (2007), *Optimizing Health: Improving the Value of Healthcare Delivery*

have irreversible and long-term negative consequences for the individual and their fundamental rights.[21] Health data thus require a higher level of protection than other types of personal data.

5. Conclusion

The rapid development of digital technology has changed how data is collected, processed, stored, shared and disclosed. Today, individuals leave digital traces with every online activity, and innovative technology such as e- and mHealth, cloud computing and Big Data allow for the collection, storage and analysis of vast amounts of data. In our globalised world, digital data transfers have become routine; however, most individuals are not aware of the potential implications, both positive and negative, of exposing their personal data, and of the complexities that govern access to and ownership of data at different stages of the process.

In order to unlock the many potential benefits of digital technology for public health, it is essential to strike a balance which protects privacy and ensures trust. Personal health data play an invaluable role in enabling research undertaken to make epidemiological progress, combating rising health inequalities and protecting public health. Therefore, EPHA believes that a strong and coherent EU framework is needed for health and care in the Digital Single Market that weighs up individual and collective health needs.

The prerequisite for effective data use and analytics is the successful and inclusive integration of digital solutions into national healthcare, coupled with ensuring digital health literacy for all end users to facilitate their assigned roles and tasks, with new technology and better data as supporting tools for transforming health systems.

[21] http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf

About EPHA

EPHA is a change agent – Europe's leading NGO advocating for better health. We are a dynamic member-led organisation, made up of public health NGOs, patient groups, health professionals, and disease groups working together to improve health and strengthen the voice of public health in Europe.

EPHA is a member of, among others, the Social Platform, the Health and Environment Alliance (HEAL), SDG Watch Europe and the Better Regulation Watchdog.

EPHA's Transparency register number is 18941013532-08.

www.epha.org

Rue de Trèves 49-51
1040 Brussels
BELGIUM

TEL: +32 (0) 2 230 30 56
FAX: +32 (0) 2 233 38 80
MAIL: epha@epha.org