USE OF SECONDARY HEALTH DATA FOR RESEARCH

The consumer checklist

WHY IT MATTERS TO CONSUMERS:

It is a prerequisite for receiving good healthcare to share your health information with your doctor. It is the primary purpose of health data collection. However, health data has a lot of value beyond this primary use. Your health information can also be used for secondary purposes such as research, health systems management and public health monitoring. Exploring ways how to maximise the secondary uses is high on the scientific and political agendas. At the European level, it manifests itself in such initiatives as the European Health Data Space, actions related to real world data uses, encouragement of data "donations" etc. While all these initiatives are driven by a promise of scientific breakthroughs, it is critical to remember that these actions are fuelled by very sensitive patient and consumer data and may therefore have a profound impact on their well-being and privacy.

OUR RECOMMENDATIONS

1 NEED FOR A SECTOR SPECIFIC REGULATION

Health data comes from varied sources: (electronic) health records, medical devices, fitness trackers, apps and social media. Multisource health data combined with the use of advanced analytics is making privacy and data protection a more complex task than just putting in place the standard protection mechanisms foreseen by the existing data protection legal framework. For example, while user consent is one of the main means to control personal data, it will in itself not provide sufficient protection regarding all possible future data uses, especially in the context of health research, where often combinations of multisource personal and non-personal data are used. Therefore, there is need for a legislation establishing:

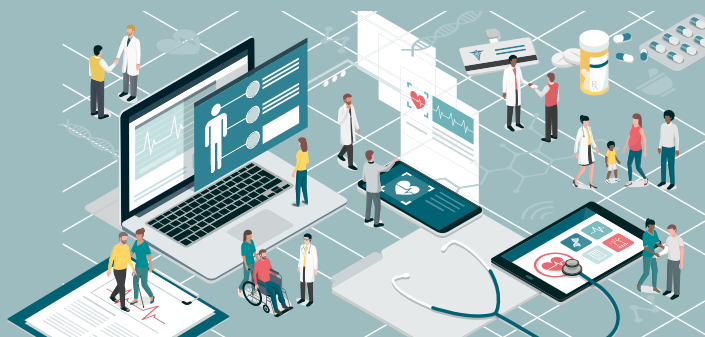
- Standards for health data anonymisation and pseudonymisation to ensure high protection of patients and consumers data;
- Quality and security standards for all information systems where health data is generated, used or stored to prevent data misuse and unauthorised access;
- Accountability, liability and redress mechanisms in case of data misuse resulting in patient or consumer harm related to health, discrimination and/or other damages;
- Strong public oversight to ensure compliance with data protection rules and other legal standards.

2 BUILDING PEOPLE-(NOT BUSINESS!) ORIENTED HEALTH-DATA SPACE

Some of the public-private partnerships in the healthcare sector are highly concerning from both a patient safety and a data protection perspective. Some big-tech companies for instance have a worrying track record when it comes to how they handle their users' data, and health data must be approached with a great caution due to its sensitivity.

Therefore, when establishing a common health data space, it is of utmost importance:

- To give priority to publicly certified service providers and ensure their full compliance with the General Data Protection Regulation, not only at the stage of contract signing but throughout the service provision.
- To make publicly certified eIDs through Electronic IDentification, Authentication and trust Services (eIDAS) the preferred method of identifying individuals when they use digital health services. Thus, associating electronic health records and other health data sources (e.g. medical device) to publicly certified eIDs should be favoured as opposed to some private initiatives (e.g. Facebook login).



3 USING REAL-WORLD DATA ONLY AS COMPLEMENTARY DATA SOURCE

When developing a new medicine, health data collected outside of randomised clinical trial – real word data – might have an added value for e.g. medicines benefit-risk assessment. However, it should not be the main evidence source to determine safety and efficacy of a drug, as it cannot replace information received through the clinical trial based on established methodology and standards. Before widely using real world data as an additional data source there is a need to:

- Determine its limitations and possibilities when it comes to generated evidence reliability.
- Develop guidelines on how to ensure quality in the context of different data sources (e.g. patient registries, electronic health records).

4 ENSURING THAT DATA ALTRUISIM ≠ DATA MANIPULATION

- Data altruism is a misleading concept which can lead to malpractice. In situations described as data altruism or data donations in which consumers would grant access to data for research with a public interest the special regime of the General Data Protection Regulation (GDPR) for collecting and controlling health data applies.
- If patients and consumers were to provide access to their data for health research under a public purpose research initiative, this should not be for commercial purposes and, if the outcome of the research then contributed to the development of medicines and treatments that are exploited commercially, conditionalities should apply to the use of the research derived from the data supplied by consumers e.g. enabling the research to be used by other parties and not licensed on an exclusive basis.
- Patients and consumers must be legally protected against misleading practices regarding initiatives by the industry which are presented as public purpose research when in reality there is a commercial intent in the exploitation of the data as a result of the commercialisation of the research outputs.

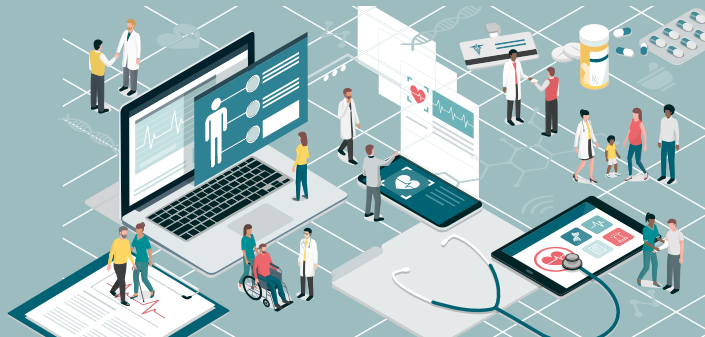
5 EDUCATING CONSUMERS, PATIENTS & HEALTHCARE PROFESSIONALS ON DIGITAL HEALTH

Healthcare digitalisation must go hand in hand with digital education and raising the level of health literacy of Europeans. 44% of Europeans do not have basic digital skills[1], while 47% have poor health literacy.[2] Inadequate knowledge of one's health and a lack of necessary skills, is a public health challenge, as well as an obstacle to a successful and consumer-oriented healthcare digitalisation. Furthermore, lack of digital skills and awareness about data protection tools of the healthcare professionals can easily put the privacy of patients at risk.

The EU and Member States should put in place mechanisms to ensure professional and educational assistance to both patients and healthcare professionals to better understand use of technologies in healthcare, their rights and obligations and how to manage health data, especially when it comes to its secondary uses.

BEUC The European Consumer Organisation

[1] https://epale.ec.europa.eu/en/resource-centre/content/digital-skills-gap-europe
[2] https://www.euro.who.int/en/health-topics/disease-prevention/health-literacy/resources



October 2020

This publication is part of an activity which has received funding under an operating grant from the European Union's Consumer Programme (2014-2020).