45th Closed Session of the Global Privacy Assembly

October 2023

Resolution on health data and scientific research

This Resolution is submitted by

SPONSOR:

- Federal Commissioner for Data Protection and Freedom of Information (BfDI), Germany

CO-SPONSORS:

- Information Commissioner's Office (ICO), United Kingdom
- Data Protection Authority (Garante per la protezione dei Dati Personali – GPDP), Italy
- National Directorate for Personal Data Protection (Agencia de Acceso a la Información Pública), Argentina
- Federal Data Protection and Information Commissioner (FDPIC), Switzerland
- Personal Data Protection Service (PDPS), Georgia
- National Data Protection Commission (Commission Nationale de l'Informatique et des Libertés – CNIL), France
- National Commission for the Protection of Personal Data (Commission nationale de contrôle et de protection des données personnelles. – CNDP), Morocco
- Privacy Protection Authority (PPA), Israel
- Office of the Information and Privacy Commissioner, Newfound and Labrador, Canada
- National Institute for Transparency, Access to Information, and Personal Data Protection (INAI), Mexico
- National Data Protection Commission (Commission nationale pour la protection des données - CNPD), Luxembourg
- Commission for Personal Data Protection, Bulgaria
- European Data Protection Supervisor (EDPS)

The 45th Global Privacy Assembly 2023,

Bearing in mind and welcoming that high quality scientific research conforming to established principles of high quality research methodology, wherever undertaken, can lead to better healthcare delivery;

Recognising the need of access to personal health data for research, innovation, economic growth technology-transfer and knowledge exchange, public health measures, and wider policy-making;

Acknowledging that the COVID-19 pandemic has shown even further the importance of building trust, confidence and transparency in the use of personal health data for the development of innovative responses and solutions to public health emergencies;

Recalling the GPA Resolution on the privacy and data protection challenges arising in the context of the COVID-19 pandemic, adopted at the 42nd Assembly (2020), and the GPA Resolution on Data Sharing for the Public Good adopted at the 43rd Assembly (2021);

Highlighting that the trusted, safe and compliant use and sharing of personal health data in line with principles of privacy by design and high standards of research quality can mitigate health risks and help develop innovative digital solutions in research, but is accompanied with risks both to specific individuals or to groups of individuals sharing characteristics associated with inappropriate data sharing or disclosure in these contexts;

Recalling that sharing of personal data, including cross-border data sharing, between governments and/or private institutions still remains an important development, but also a key challenge regarding privacy and data protection while addressing urgent public interests;

Recognising that the processing of health data, which are particularly sensitive, is subject to strict international, regional and national data protection rules, and furthermore that additional requirements may apply to genetic/genomic health information due to unique privacy considerations;

Underlining the importance of collaboration among the GPA community and with local users and sectoral regulators of health data use in research to address the data protection and privacy risks arising from an increase in the amount and volume of sharing and processing of personal health data and to support the effective, safe and compliant sharing of health data in the public interest;

Acknowledging the approach that respecting human rights and human dignity are at the heart of high quality scientific research involving ethical research into human subjects. Legal regulations must effectively ensure the protection of the right to informational self-determination of data subjects;

Underlining that the following principle applies: The higher the risk for data subjects, which is often associated with extensive and specific use of personal data, the higher protection of data subjects through appropriate safeguards and measures is required;

Emphasizing that basic safeguards and measures to protect the health data must always be implemented. These could include, as appropriate, anonymisation, to prevent the re-identification of data subjects, or encryption, de-identification and pseudonymisation by a trusted body to protect the personal data;

Highlighting that evaluations based on case data particularly deeply affect the rights and freedoms of the data subjects when data sets from different sources are linked and that data linking involving genetic/genomic health information may impact indigenous and other communities with shared genetic heritage, and not just individuals;

Affirming that patient confidentiality is a key principle of high quality medical practice, and that this aligns well with individuals' privacy rights. This principle is also an important element in building trust and confidence in the use of personal health data, and should therefore be protected by users and regulators of personal health data;

Further affirming that providing timely, easily understandable and accessible transparency information about the processing of health data to data subjects, regulators and the wider users of health research are important principles in effective privacy by design and in building trust and confidence in the use of health data in research;

Underlining that data protection authorities must be able to comprehensively and effectively monitor and enforce compliance with data protection requirements; and wherever possible should also seek to provide advice and guidance to all concerned on the safe and compliant use of personal health data;

Emphasizing the importance of incentivising the development of privacy enhancing technologies (PETs), which may be crucial for protecting health data used for research, and the importance of Data Protection Supervisory Authorities and all stakeholders being well educated about the variety of PETs available, including the advantages and risks for each PET;

The 45th Global Privacy Assembly therefore resolves to:

1. Call upon all decision makers, stakeholders and parties, which are involved in collecting and processing health data of individuals for scientific purposes or in a research context, to embrace privacy by design as a key element within research project design that aligns well with long established principles of high quality and ethical research design, and to identify and implement appropriate requirements and safeguards and PETs continuously from the outset, including those mentioned above, in their respective health data processing operations. Such implementation should be reassessed and adjusted accordingly, by regular audits and reviews with regard to the suitability and effectivity of data protection measures and safeguards, which have been put in place. Where and as far as necessary, those measures and safeguards should be adapted in order to continue to ensure an appropriate level of data protection.

2. Invite the GPA Data Sharing Working Group to further reflect on addressing the collection and processing of health data for scientific purposes or in a research context, while at the same time indicating the principles, rights and relevant safeguards to be applied in the context of sharing of data for the public good.

Explanatory note:

Scientific research with health data, including with information on the health status of individuals or information about an individual's health inferred from non-health data, can serve to gain insights into the causes of diseases, to develop efficient therapies and to improve treatment options.

It is therefore in the essential interest of the general public and should be promoted in the best possible way in the pursuit of these objectives. However, it should be noted that the relevant data categories are protected by national and international law in a special way and are subject to a particularly high level of protection. Improper use of sensitive health data can lead to serious harms, such as social stigmatisation, medical identity theft, financial loss, mental anguish or discrimination for the data subjects, for example in the labour and insurance markets.

With the well-founded trust of the persons concerned in compliance with ethical, legal and technical standards, their motivation to support research grows. It is therefore essential for citizens to be able to trust that their personal data will be processed in accordance with the data protection requirements and while safeguarding their right to informational self-determination. This is also the reason why data protection is a prerequisite for human-centred scientific research with health data.

It is the task of the legislator to enable research in the public interest with health data, but also to define its limits and to safeguard the fundamental rights and interests of the data subjects. The legislator must not completely shift the burden of navigating these complex issues onto the individual responsibility of patients and the researchers.

If a legal provision is intended to be the legal basis for data processing for research purposes, it must be precise and specific, and it must in any case effectively guarantee the protection of the right to informational self-determination of the data subjects. Such a provision may enable or facilitate data compliant research in the use of data from other sources, such as treatment data from hospitals, medical registers or other research projects. However, a legal basis for the processing of health data must contain sufficient and adequate measures to protect the fundamental rights and interests of data subjects.

Insofar as the research purpose can be achieved with anonymised data, only anonymised data should be processed. There are high demands to be taken into account with regard to the anonymisation of personal data. In cases where full anonymisation is not possible in order to achieve the research purpose, effective measures of pseudonymisation with protections against re-identification designed according to the research context, shall be implemented. In addition, technical and organisational safeguards must be designed in accordance with the requirements of the state of the art for health data, including those for pseudonymisation and encryption of the data, and other forms of Privacy by Design or PETs mechanisms which ensure data minimization and enhanced protection (such as Federated Learning, Multi Party Computation, Homomorphic Encryption, etc.).

Data protection supervisory authorities must be able to fully monitor and enforce compliance with data protection regulations in the area of processing personal health data in a research context. They must also be empowered to take appropriate enforcement measures vis-à-vis public authorities and private bodies. This further includes the possibility to order the immediate implementation of measures or even the cessation of specific data processing operations, which fail to meet necessary and adequate data protection standards. For this purpose, data protection authorities need to be equipped with sufficient human and financial resources as well as with necessary technological means.