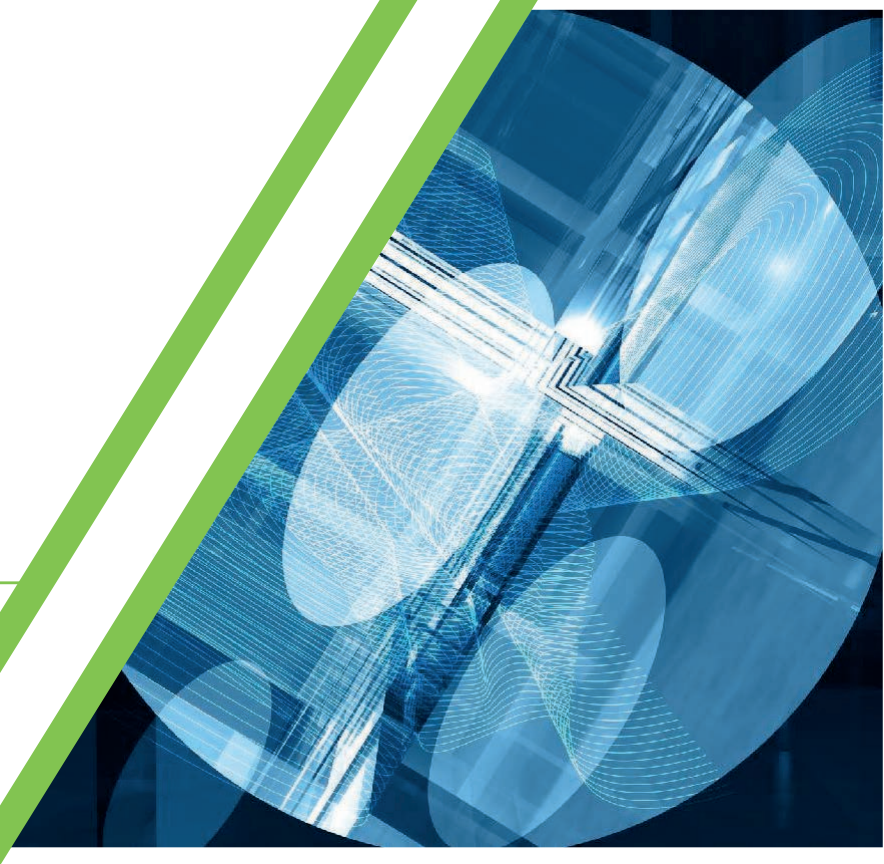
Recommendation of the Council on Health Data Governance



OECD Legal Instruments

OECD

BETTER POLICIES FOR BETTER LIVES

Please cite this document as:
OECD, *Recommendation of the Council on Health Data Governance*, OECD/LEGAL/0433

Series: OECD Legal Instruments

Date(s)

Adopted on 13/12/2016

Background Information

The Recommendation on Health Data Governance was adopted by the OECD Council on 13 December 2016 on the proposal of the Health Committee and Committee on Digital Economy Policy. This Recommendation recognises that many OECD Members lack a coordinated public policy framework to guide health data use and sharing practices, so as to protect privacy, enable efficiencies, promote quality and foster innovative research. Its main objective is to recommend that Adherents establish and implement a national health data governance framework to encourage the availability and use of personal health data to serve health-related public interest purposes while also promoting the protection of privacy, personal health data and data security. The Recommendation aims to support greater harmonisation among the health data governance frameworks of Adherents, so that more countries are able to benefit from statistical and research uses of data in which there is a public interest, and so that more countries can participate in multi-country statistical and research projects, while protecting privacy and data security.

THE COUNCIL,

HAVING REGARD to Article 5 b) of the Convention on the Organisation for Economic Co-operation and Development of 14 December 1960;

HAVING REGARD to the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [C(80)58/FINAL as amended by C(2013)79], the Recommendation of the Council on Human Biobanks and Genetic Research Databases [C(2009)119] and the Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity [C(2015)115];

NOTING the OECD report *Health Data Governance: Privacy, Monitoring and Research* (OECD, 2015);

RECOGNISING that access to, and the processing of, personal health data can serve health-related public interests and bring significant benefits to individuals and society;

RECOGNISING that health systems are increasingly affected by a growing volume of personal health data in electronic form, including electronic health and administrative records; that such data are often held in silos by the organisations that have collected them and by governmental authorities, such as health ministries and statistical agencies; and that when the secure transfer, linkage and analysis of health data occurs, then the value of the data to serve health-related public interest purposes increases significantly.

RECOGNISING that public trust and confidence in the protection of personal health data must be maintained if the benefits achievable through its processing are to be realised; and that governments have a role in fostering compliance with privacy laws and policies.

RECOGNISING that personal health data, being sensitive in nature and subject to ethical standards and the principle of medical confidentiality, require a particularly high level of protection and that technological developments can both enable the privacy protective use of personal health data and also introduce new risks to privacy and data security;

RECOGNISING that achieving these benefits requires the careful development and application of robust, context appropriate, privacy protective health data governance frameworks that require the identification and management of privacy and security risks;

RECOGNISING that although Members and non-Members adhering to this Recommendation (hereafter the "Adherents") are investing in health data infrastructure and that considerable progress is being made to achieve co-ordinated health data governance frameworks, the many differences in the availability of, access to and use of personal health data both within and across national borders must be addressed; and

CONSIDERING that, while there are differences in their domestic laws, effectively safeguarding the public interest is an important function of governments; that health data governance is not only the domain of central governments but that it encompasses all levels of government, where different mandates apply in different countries; and that this Recommendation is accordingly relevant to all levels of government.

On the proposal of the Health Committee and the Committee on Digital Economy Policy:

I. **AGREES** that this Recommendation applies to the access to, and the processing of, personal health data for health-related public interest purposes, such as improving health care quality, safety and responsiveness; reducing public health risks; discovering and evaluating new diagnostic tools and treatments to improve health outcomes; managing health care resources efficiently; contributing to the progress of science and medicine; improving public policy planning and evaluation; and improving patients' participation in and experiences of health care.

II. **AGREES** that for the purpose of this Recommendation the following technical terms require a brief description to support a common understanding:

- “Personal health data” means any information relating to an identified or identifiable individual that concerns their health, and includes any other associated personal data.
- “Processing personal health data” means all data-related operations involving personal health data such as data collection, use, disclosure, storage, recording, editing, retrieval, transfer, sharing, linkage or combining, analysis, and erasure.
- “De-identification” means a process by which a set of personal health data is altered, so that the resulting information cannot be readily associated with particular individuals. De-identified data are not anonymous data. “Re-identification” means a process by which information is attributed to de-identified data in order to identify the individual to whom the de-identified data relate.

III. RECOMMENDS that governments establish and implement a national health data governance framework to encourage the availability and use of personal health data to serve health-related public interest purposes while promoting the protection of privacy, personal health data and data security. Such a health data governance framework should provide for:

1. **Engagement and participation**, notably through public consultation, of a wide range of stakeholders with a view to ensuring that the processing of personal health data under the framework serves the public interest and is consistent with societal values and the reasonable expectations of individuals for both the protection of their data and the use of their data for health system management, research, statistics or other health-related purposes that serve the public interest.
2. **Co-ordination within government and promotion of cooperation among organisations processing personal health data, whether in the public or private sectors**. This cooperation should:

    i. Encourage common data elements and formats; quality assurance; and data interoperability standards; and

    ii. Encourage common policies and procedures that minimise barriers to sharing data for health system management, statistics, research and other health-related purposes that serve the public interest while protecting privacy and data security.

3. **Review of the capacity of public sector health data systems used to process personal health data to serve and protect the public interest.** Such review should include:

    i. Data availability, quality, fitness for use, accessibility, as well as privacy and data security protections.

    ii. Elements of data processing that are permitted for health system management, research, statistics or other health-related public interest purposes, subject to appropriate safeguards, particularly dataset transfers and the linkage of dataset records.

4. **Clear provision of information to individuals.** Such provision should ensure that:

    i. Where personal health data are collected from individuals, information about the processing of their personal health data, including possible lawful access by third parties, the underlying objectives behind the processing, the benefits of the processing, and its legal basis is disclosed in clear, accurate, easily understandable and conspicuous terms.

    ii. Individuals are notified in a timely manner of any significant data breach or other misuse of their personal health data. Where individual notification is not practicable then notification may be made by effective public communication.

5. **Informed consent and appropriate alternatives.**

    i. Consent mechanisms should provide:

a. Clarity on whether individual consent to the processing of their personal health data is required, and, if so, the criteria used to make this determination; what constitutes valid consent and how consent can be withdrawn; and lawful alternatives and exemptions to requiring consent, including in circumstances where obtaining consent is impossible, impracticable or incompatible with the achievement of the health-related public interest purpose, and the processing is subject to safeguards consistent with this Recommendation.

b. That, where the processing of personal health data is based on consent, such consent should only be valid if it is informed and freely given, and if individuals are provided with clear, conspicuous and easy to use mechanisms to provide or withdraw consent for the future use of the data.

ii. Where the processing of personal health data is not based on consent, to the extent practicable, mechanisms should provide that:

a. Individuals should be able to express preferences regarding the processing of their personal health data, including not only the ability to object to processing under certain circumstances but also the ability to actively request that their personal health data be shared for research or other health-related public interest purposes.

b. If data processing objections or requests cannot be honoured, then individuals should be provided with the reasons why this is the case including the relevant legal basis.

6. **Review and approval procedures, as appropriate, for the use of personal health data for research and other health-related public interest purposes**. Such review and approval procedures should:

i. Involve an evidence-based assessment of whether the proposed use is in the public interest;

ii. Be robust, objective and fair;

iii. Operate in a manner that is timely and promotes consistency of outcomes;

iv. Operate transparently whilst protecting legitimate interests; and

v. Be supported by an independent multi-disciplinary review conducted by those with the expertise necessary to evaluate the benefits and risks for individuals and society of the processing, and risk mitigation.

7. **Transparency, through public information mechanisms which do not compromise health data privacy and security protections or organisations' commercial or other legitimate interests.** Public information should include the following elements:

i. The purposes for the processing of personal health data, and the health-related public interest purposes that it serves, as well as its legal basis.

ii. The procedure and criteria used to approve the processing of personal health data, and a summary of the approval decisions taken, including a list of the categories of approved data recipients.

iii. Information about the implementation of the health data governance framework and how effective it has been.

8. **Maximising the potential and promoting the development of technology** as a means of enabling the availability, re-use and analysis of personal health data while, at the same time, protecting privacy and security and facilitating individuals' control of the uses of their own data.

9. **Monitoring and evaluation mechanisms.** Such mechanisms should:

i. Assess whether the uses of personal health data have met the intended health-related public interest purposes and brought the benefits expected from such uses and whether any negative consequences of such uses have occurred, including failures to comply with national requirements for the protection of privacy, personal health data and data security; data breaches and data misuses; and feed the results of such assessment into a process of continuous improvement, including through:

   a. Periodic review of developments in personal health data availability, the needs of health research and related activities, and public policy needs; and

   b. Periodic assessment and updating of policies and practices to manage privacy, protection of personal health data and security risks relating to personal health data governance.

ii. Encourage those processing personal health data to periodically review and assess the capabilities, reliability and vulnerabilities of the technologies they use.

10. **Establishment of appropriate training and skills development in privacy and security measures for those processing personal health data,** that are in line with prevailing standards and data processing techniques.

11. **Implementation of controls and safeguards.** These should:

i. Provide clear and robust lines of accountability for personal health data processing, accompanied by appropriate mechanisms for audit.

ii. Establish requirements that personal health data can only be processed by, or be the responsibility of, organisations with appropriate data privacy and security training for all staff members, commensurate with their roles and responsibilities in relation to processing personal health data and consistent with any applicable professional codes of conduct.

iii. Encourage organisations processing personal health data to designate an employee or employees to coordinate and be accountable for the organisation's information security programme, including informing the organisation and its employees of their legal obligations to protect privacy and data security.

iv. Include formal risk management processes, updated periodically that assess and treat risks, including unwanted data erasure, re-identification, breaches or other misuses, in particular when establishing new programmes or introducing novel practices.

v. Include technological, physical and organisational measures designed to protect privacy and security while maintaining, as far as practicable, the utility of personal health data for health-related public interest purposes. Such measures should include:

   a. Mechanisms that limit the identification of individuals, including through the de-identification of their personal health data, and take into account the proposed use of the data, while also allowing re-identification where approved. Re-identification may be approved to conduct future data analysis for health system management, research, statistics, or for other health-related public interest purposes; or to inform an individual of a specific condition or research outcome, where appropriate.

   b. Agreements, when sharing personal health data with third parties for processing that help to maximise the benefits and manage the risks while maintaining the utility of personal health data. Such agreements should specify arrangements for the secure transfer of data and include appropriate means to effectively sanction non-compliance.

   c. Where practicable and appropriate, considering alternatives to data transfer to third parties, such as secure data access centres and remote data access facilities.

d. Robust identity verification and authentication of individuals accessing personal health data.

12. **Require organisations processing personal health data to demonstrate that they meet national expectations for health data governance.** This may include establishment of certification or accreditation of organisations processing personal health data, in so far as these certifications or accreditations help to implement standards for the processing of personal health data or demonstrate capacity to meet recognised governance standards.

IV. **RECOMMENDS** that governments support transborder co-operation in the processing of personal health data for health system management, research, statistics and other health-related purposes that serve the public interest subject to safeguards consistent with this Recommendation. To that effect, governments should:

i. Identify and remove barriers to effective cross-border cooperation in the processing of personal health data for health-related public interest purposes in a manner consistent with protecting privacy and data security, in light of all the circumstances.

ii. Facilitate the compatibility or interoperability of health data governance frameworks.

iii. Promote continuous improvement through the sharing of outcomes and best practices in the availability and use of personal health data for health system management, research, statistics and other health-related purposes that serve the public interest.

V. **RECOMMENDS** that governments engage with relevant experts and organisations to develop mechanisms consistent with the principles of this Recommendation that enable the efficient exchange and interoperability of health data whilst protecting privacy, including, where appropriate, codes, standards and the standardisation of health data terminology.

VI. **ENCOURAGES** non-governmental organisations to follow this Recommendation when processing personal health data for health-related purposes that serve the public interest.

VII. **INVITES** the Secretary-General to disseminate this Recommendation.

VIII. **INVITES** Adherents to disseminate this Recommendation at all levels of government.

IX. **INVITES** non-Adherents to take account and to adhere to this Recommendation.

X. **INSTRUCTS** the Health Committee, in co-operation with the Committee on Digital Economy Policy, to:

a) Serve as a forum to exchange information on progress and experiences with respect to the implementation of this Recommendation, and;

b) Monitor the implementation of this Recommendation and report to the Council within five years of its adoption and thereafter as appropriate.

Adherents*

OECD Members	Non-Members
Australia	
Austria	
Belgium	
Canada	
Chile	
Czech Republic	
Denmark	
Estonia	
Finland	
France	
Germany	
Greece	
Hungary	
Iceland	
Ireland	
Israel	
Italy	
Japan	
Korea	
Latvia	
Luxembourg	
Mexico	
Netherlands	
New Zealand	
Norway	
Poland	
Portugal	
Slovak Republic	
Slovenia	
Spain	
Sweden	
Switzerland	
Turkey	
United Kingdom	
United States	

*Additional information and statements are available in the Compendium of OECD Legal Instruments: http://legalinstruments.oecd.org

About the OECD

The OECD is a unique forum where governments work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD Member countries are: Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Latvia, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Union takes part in the work of the OECD.

OECD Legal Instruments

Since the creation of the OECD in 1961, around 450 substantive legal instruments have been developed within its framework. These include OECD Acts (i.e. the Decisions and Recommendations adopted by the OECD Council in accordance with the OECD Convention) and other legal instruments developed within the OECD framework (e.g. Declarations, international agreements).

All substantive OECD legal instruments, whether in force or abrogated, are listed in the online Compendium of OECD Legal Instruments. They are presented in five categories:

- **Decisions**: OECD legal instruments which are legally binding on all Members except those which abstain at the time of adoption. While they are not international treaties, they entail the same kind of legal obligations. Adherents are obliged to implement Decisions and must take the measures necessary for such implementation.

- **Recommendations**: OECD legal instruments which are not legally binding but practice accords them great moral force as representing the political will of Adherents. There is an expectation that Adherents will do their utmost to fully implement a Recommendation. Thus, Members which do not intend to do so usually abstain when a Recommendation is adopted, although this is not required in legal terms.

- **Declarations**: OECD legal instruments which are prepared within the Organisation, generally within a subsidiary body. They usually set general principles or long-term goals, have a solemn character and are usually adopted at Ministerial meetings of the Council or of committees of the Organisation.

- **International Agreements**: OECD legal instruments negotiated and concluded within the framework of the Organisation. They are legally binding on the Parties.

- **Arrangement, Understanding and Others**: several ad hoc substantive legal instruments have been developed within the OECD framework over time, such as the Arrangement on Officially Supported Export Credits, the International Understanding on Maritime Transport Principles and the Development Assistance Committee (DAC) Recommendations.