Recommendation of the OECD Council on Health Data Governance

THE NEXT GENERATION of **HEALTH REFORMS**

OECD Health Ministerial Meeting

17 January 2017

OECD

BETTER POLICIES FOR BETTER LIVES

Introduction

Health data are an increasingly essential ingredient to enhance health system performance and health care quality, and contribute to scientific discoveries that improve medical treatments and save lives. As the volume and variety of data increase, so does the ability to derive further information from these data, particularly when they are linked and merged across the many organisations that collect them, such as hospitals, physician offices, pharmacies, laboratories, bio-banks, statistical offices and medical device and app businesses.

Health data are also sensitive in nature and fostering data sharing and use increases the risk of data loss or misuse that can bring personal, social and financial harms to individuals and can diminish public trust in health care providers and governments. Such risks must therefore be appropriately mitigated and managed.

The breadth and scale of data collection practices has also given rise to new challenges in the implementation of existing data protection standards and procedures that need to be addressed, such as consent to personal data collection and use. It has also highlighted the importance of complementing legal data protection through education and awareness raising, skills development, and the promotion of technical measures so that the potential benefits of new analytic techniques may be achieved.

This Recommendation of the OECD Council calls upon countries to develop and implement health data governance frameworks that secure privacy while enabling health data uses that are in the public interest. It is structured according to twelve high-level principles, ranging from engagement of a wide range of stakeholders, to effective consent and choice mechanisms to the collection and use of personal health data, to monitoring and evaluation mechanisms. These principles set the conditions to encourage greater cross-country harmonisation of data governance frameworks so that more countries are able to use health data for research, statistics and health care quality improvement, as well as for international comparisons.

This Recommendation was adopted by the OECD Council on 13 December 2016 and was welcomed by OECD Health Ministers at their meeting in Paris on 17 January 2017. It follows from a mandate given by Health Ministers in 2010, calling on the OECD to support countries in making better use of health data to improve health care quality. Since then, the OECD has published several reports illustrating that too many countries still lack a co-ordinated public policy framework to guide health data use and sharing practices. The Recommendation is the product of a multi-stakeholder effort. It has been jointly produced by the OECD Committee on Digital Economy Policy, which supports the development and promotion of policies to stimulate the growth of an accessible, innovative, open and trusted digital economy for sustained prosperity and wellbeing, and the OECD Health Committee, which supports the development and promotion of policies to strengthen health systems and improve health system performance. It has involved the advice of experts in privacy, law, ethics, health, government policy, research, statistics and IT and extensive consultations with civil society (CSISAC), Business and Industry (BIAC), OECD Committees and the OECD Secretariat.

This informal advisory Expert Group was co-chaired by Ms. Jennifer Stoddart, former Privacy Commissioner of Canada, (Canada) and Dr. Päivi Hämäläinen, Leading Expert, Department for Health and Social Care Systems, National Institute for Health and Welfare (THL), (Finland). Proposed revisions were developed by a drafting group including the OECD Secretariat, the Chairs, Prof. Bartha Knoppers (Canada), Dr. Mark Taylor, and Mr. David Smith (UK).

OECD Recommendations are not legally binding, but practice accords them great moral force as representing the political will of Member countries and there is an expectation that Member countries will do their utmost to fully implement a Recommendation. The OECD will monitor progress in the implementation of this Recommendation.

This Recommendation represents a major achievement. It highlights the strong commitment of countries to make better use of health data, to foster international cooperation in health research and ultimately to improve health system performance and outcomes for people, while promoting and protecting the fundamental values of privacy and individual liberties.

Recommendation of the OECD Council on Health Data Governance

THE COUNCIL,

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

HAVING REGARD to the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Trans-border 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. S**uch 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 cooperation 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 cooperation 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.

Annex 1: Background and Rationale for the Recommendation of the OECD Council on Health Data Governance

This section is a background note to the Recommendation of the OECD Council on Health Data Governance. It is intended to assist the reader in understanding the context of the elements within the Recommendation. It is presented for information only and it does not constitute part of the Recommendation.

Introduction

The Recommendation of the OECD Council on Health Data Governance (hereafter the "Recommendation") was jointly developed by the OECD Committee on Digital Economy Policy (CDEP) advised by its Working Party on Security and Privacy in the Digital Economy (SPDE), and the OECD Health Committee (HC) advised by its Health Care Quality Indicators Expert Group (HCQI).

Following discussion and approval by both Committees, the draft Recommendation was adopted by the OECD Council in December 2016 and welcomed by Ministers at the meeting of the HC at Ministerial level in January 2017.

Rationale for developing the Recommendation

The populations in OECD Members are ageing with increasing shares of people are living longer, often with multiple chronic and disabling conditions. At the same time, the health sector is one of the most rapidly growing sectors of the economy but needs to adapt to changes in demand, distribution, and cost of treatment, which have important implications for how care is organised and provided, where new treatment innovations can be expected, as well as rising costs. The increasing pressures to respond to growing needs while containing expenditures are driving health systems toward greater use of health data to assess the comparative-effectiveness of therapies and services and inform policy. Health data are necessary to improve the quality, safety and patient-centeredness of health care services and to support scientific innovation, the discovery and evaluation of new treatments and to redesign and evaluate new models of health service delivery.

The volume of personal health data in electronic form is already very large and is growing with technological progress including electronic health and administrative records; behavioural and environmental monitoring devices and apps; and bio-banking and genomic technologies. Health data are principally generated as part of the provision and reimbursement of health care services, including data from primary health care, hospital, pharmacy, laboratory, long-term care and other services, as well as from scientific, business and statistical sources including surveys, insurance claims, clinical studies, social media, and health monitoring software. Health data are also increasingly generated by consumers using their own personal digital devices to monitor their health, such as, measuring their insulin levels or the number of steps they take each day.

Often the data are held in silos by the organisations that have collected them and by governmental authorities, such as health ministries and statistical agencies. However, when such data are linked and analysed, then an exponential gain in information value can be attained to serve the health related public

interest. Examples include improving diagnosis, particularly for rare diseases; identifying optimal responders to treatment and personalising care for better patient outcomes; detecting unsafe health care practices and treatments; rewarding high quality and efficient health care practices; detecting fraud and waste in the health care system; assessing the long-term effects of medical treatments; and discovering and evaluating new health care treatments and practices.

An important impediment to harnessing the benefits of the health data analysis is 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. While all OECD Members are investing in health data, a 2013 OECD study uncovered significant cross- country differences in health data availability and use.[1]

Several Members have made significant progress in this field and have implemented innovative practices that enable data processing, while, at the same time, protecting privacy and data security. However others have fallen behind with both insufficient data and restrictions that limit access to and further processing of data, even by government itself. The 2013 study highlighted cases where health data processing, despite the potential of significant beneficial returns, may be prevented or may take years to approve due to legal and other uncertainties.

At the same time, the scale, capabilities and methodologies of data gathering, aggregation, and analysis are radically evolving. Emerging technologies including Big Data analytics can, for example, utilise enhanced computing power to process broad ranges of data in real time, that could support patient-care and further the discovery of disease markers and disease-specific solutions. Examples of beneficial uses of Big Data are emerging, including decision-support tools developed for clinicians treating cancer patients that are based on analysis of huge volumes of data emerging from personalised medicine for cancer care; research involving linked health care data at the population level to discover inequalities in access to treatment; rapid monitoring of population-level health insurance data to detect and address the underuse, overuse and misuse of therapies; and analysis of population-level clinical data to assess the quality and efficiency of health care guidelines for clinicians to ensure that guidelines are being followed and are producing expected results.[2] As we consider technologies that can enhance analytics across broader and more granular data, uncertainties emerge about how the potential benefits of such analytic techniques can be achieved in the context of the implementation of existing data protection standards and procedures, in particular, consent, data minimisation and purpose-limited retention of data.

Rapid progress in information technology and processing, and associated research techniques and methodologies, may also allow for innovative solutions enabling limited access to data under secure conditions with increased opportunities for transparency, accountability and audit. Thus, there will be an on-

[1] See the 2013 OECD report on Strengthening Health Information Infrastructure for Health Care Quality Governance: Good Practices, New Opportunities and Data Privacy Protection Challenges (hereafter the "2013) study") available at http://www.oecd.org/publications/strengthening-health-information-infrastructure-for-health-care-quality-governance-9789264193505-en.htm.

[2] OECD (2015), Data-Driven Innovation for Growth and Well-Being, Chapter 8: The Evolution of Health Care in a Data-Rich Environment. OECD Publishing, Paris.

going need to evaluate the impact of new technologies on health data availability, use and the protection of health data privacy and security.

The importance of effective, global and national approaches to governance of the processing of personal health data has never been greater if the potential for society to benefit from the use of health data are to be realised. There are legal instruments that promote coordinated frameworks for the protection of privacy in the use of personal data in general, such as 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] (hereafter the "Privacy Guidelines"), the European Union Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data[3], the upcoming Regulation (EU) 2016/679 ("General Data Protection Regulation" (GDPR)[4], Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS No 108 and its Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows No 181, and the APEC Cross-border Privacy Rules. There remains, however, a need for international consensus about the framework conditions within which health data can be appropriately governed to enable health data processing to take place both domestically and transnationally. Such health data governance frameworks require a whole of government approach, given that the public interests served span the domains of health, justice, industry, science, innovation and finance.

There are risks and benefits from health data processing at both the individual and societal levels. The maintenance of a confidential health care system is fundamental to effective individual care and treatment and to public health. It is crucial to the relationship of trust between a patient and a healthcare professional. Data security breaches or misuses of personal health data can undermine the trustworthiness and integrity of health care systems. At the same time, a failure to support appropriate collection, linkage, use and further processing may undermine the conditions necessary for public health and individual well-being. The under-use of health data will limit the effective and efficient development and delivery of healthcare. Appropriate reconciliation of these risks and benefits is necessary if the interests of both individuals and societies are to be best served. This requires transparency, an understanding of the reasonable expectations of individuals, and the development of a shared view of how best to serve the public interest in both the protection of health data privacy and in the benefits to individuals and to societies from health data availability and use.

A follow-on study was pursued in 2013/14 to uncover and document promising health data governance practices[5]. Twenty-two countries[6] participated in the 2015 study which included detailed

[3] Directive 95/46/EC of The European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L L 281 , 23/11/1995 P. 0031 – 0050.

[4] 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, p. 1–88.

[5] See the 2015 OECD report *Health Data Governance: Privacy, Monitoring and Research* (hereafter the "2015 study") available at http://www.oecd.org/publications/health-data-governance-9789264244566- en.htm. The 2015 study results were discussed at an OECD workshop, Health Data Governance – Strategies to Maximise Societal Benefits and Minimise Risks, held on 20 May 2015.

information about national health data and its governance, provided by governments and national experts through surveys and personal interviews. The study was widely reviewed by experts in health data development and health data governance within countries and was reviewed by the HC and the CDEP Working Party on Security and Privacy in the Digital Economy (SPDE).

The following key conclusions emerged from the 2015 study:

- there is a **wide variation across surveyed countries in the development and use of health data**: elements of data processing, such as data transfers between organisations processing health data and the linkage of data from different organisations, are permitted for statistical and research purposes subject to safeguards in some countries but they are restricted or prohibited in others;

- a **health data governance framework with mechanisms and best practices** to protect health data privacy at all stages of data systems development and use would be the best way forward to create an environment within which the benefits of safe data use can be realised. To be effective, such a framework should protect individuals and build trust in governments and health care systems, while enabling health data processing that is in the public interest;

- **eight key health data governance mechanisms** were identified to maximise benefits to patients and to societies from the collection, linkage and analysis of health data while, at the same time, minimise risks to the privacy of patients and to the security of health data:

    1. The health information system supports the monitoring and improvement of health care quality and system performance, as well as research innovations for better health care and outcomes.

    2. The processing of data for public health, research and statistical purposes are permitted, subject to safeguards specified in the legislative framework for data protection.

    3. The public is consulted upon and informed about the collection and processing of personal health data, including regular, clear and transparent public information about the data collected and processed, the benefits and risks of the processing, and the risk mitigations in place.

    4. A certification or accreditation process for the processing of health data for research and statistics is implemented.

    5. The project approval process is fair and transparent and decision-making is supported by an independent, multidisciplinary project review body.

    6. Best practices in data de-identification are applied to protect patient data privacy.

[6] Twenty-one OECD Members and Singapore took part in the study.

7. Best practices in data security and management are applied to reduce re-identification and breach risks.

8. Governance mechanisms are periodically reviewed at an international level as new data sources and new technologies are introduced.

- **international collaboration toward common best practices is essential** to enable all countries to safely benefit from health data and to support the production of multi-country statistics, research and other uses of data that serve the public interest.

The Recommendation included in this document follows up on these conclusions and presents a set of recommendations, for Members and non-Members adhering to it (hereafter "Adherents") to establish and implement a national health data governance framework for the processing of personal health data[7] for health system management, research, statistics and other health-related purposes that serve a public interest.

Scope and objective of the Recommendation

The Recommendation is intended to:

- encourage the availability and use of personal health information, to the extent that this enables significant improvements in health, health care quality and performance and, thereby, the development of healthy societies whilst, at the same time, continuing to promote and protect the fundamental values of privacy and individual liberties;

- promote the use of personal health data for public policy objectives, while maintaining public trust and confidence that any risks to privacy and security are minimized and appropriately managed;

- 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 Recommendation recognises that personal health data are processed by national and sub-national levels of government for a range of public interests including, but not limited to, research and statistics and recommends practices that promote the privacy-protective use of health data.

Personal health data are also processed by profit or not-for-profit non-governmental organisations, such as health and social care providers, insurance providers, research institutes, universities, and other businesses collecting health information including pharmacies, providers of health monitoring devices, app developers and others. Accordingly, this Recommendation also encourages that non-governmental organisations and

[7] A dataset of personal health data may include other personal data, such as birthdate, socio-economic status, ethnic origin, marital status or other personal characteristics necessary for administrative, statistical or research purposes.

companies involved in processing personal health data in the public interest follow, as appropriate, this Recommendation.

Finally, the Recommendation contains a provision by which the Council instructs the HC and CDEP to monitor progress and policy development in the implementation to the Recommendation and report thereon to the Council no later than five years following its adoption and regularly thereafter to ensure that the Recommendation remains relevant.

Process to develop the Recommendation

In response to the findings of the 2013 and 2015 studies, the HC at its 9-10 December 2014 meeting approved the initiation of a process to develop the Recommendation, subject to the participation of the CDEP and asked its Health Care Quality Indicators Expert Group (HCQI) to advise on this work. The SPDE discussed the proposal at its December 2014 meeting and expressed its support for moving ahead recognising, however, the need to establish an informal expert Advisory Group to guide and further scope this work. CDEP agreed to the development of this Recommendation with the HC on 24 June 2014 and asked its Working Party on Security and Privacy in the Digital Economy (SPDE) to undertake the work.

A multi-disciplinary Advisory Expert Group (AEG) was established in the summer of 2015 to provide advice at all stages of the development of the draft Recommendation. It was co-chaired by representatives of HCQI and SPDE. The AEG included experts in health, law, privacy, statistics, research, policy and IT from government, academia, industry and civil society. Three teleconferences and one in-person meeting took place in 2015.

A progress report on the development of the draft Recommendation was provided to the HC at their meeting of 3-4 December 2015, to the CDEP at their meeting of 2-4 December 2015 and to the SPDE at their meeting of 2 December 2015. An oral progress report was provided to the HCQI at their meeting of 9-10 November 2015.

The AEG co-chairs, the OECD Secretariat and expert consultants prepared the draft Recommendation considering the comments received from HC, SPDE and HCQI delegates; the input provided by the AEG and structured it following the guidance of the OECD Directorate for Legal Affairs.

The Recommendation builds on existing OECD Recommendations, particularly the Privacy Guidelines, which sets out eight guiding principles for the protection of privacy and the transborder flow of personal data that OECD Members apply. The Privacy Guidelines is expressly mentioned in the preamble of the Recommendation and the operative part of the Recommendation provides for the specific privacy aspects applicable to health data. The text also considered the OECD Recommendation on Digital Government Strategies [C(2014)88] which suggests governments develop and implement digital government strategies that support the creation of a data driven culture in the public sector with the view to improve administration and service delivery, as well as public policy planning and impact (including in the health domain).

The Recommendation does not refer to the legal instruments of other international organisations or to the specific work of NGOs as not all Members may have endorsed these instruments. It also does not refer to broad principles or to human rights that are already covered by existing legal instruments.

The Recommendation uses accessible language that minimises the use of technical or profession-specific terminology in order to communicate clearly with a broad audience. Where technical terminology is unavoidable, accessible and concise definitions are proposed. Specific technologies are not mentioned to ensure that the Recommendation stands the test of time.

Specifically, 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-identification can include a range of mechanisms (e.g., data suppression, data coding and aggregation). The question of whether personal health data sets have been sufficiently de-identified can be evaluated against a range of factors, including the applicable organizational structures, security measures and level of time and effort needed to re-identify the data.[8] De-identified data are not anonymous data.

HC, SPDE and HCQI delegates provided comments on the draft Recommendation by written procedure in May 2016. A revised draft was then provided for discussion during the HC meeting of 28-29 June 2016 and the CDEP meeting of 24 June 2016. Delegates provided further written comments on the draft Recommendation in July-August 2016.

The Public Governance and Territorial Development Directorate (GOV) provided written comments and supported the drafting of the Recommendation which duly takes into consideration the Recommendation of the Council on Digital Government Strategies [C(2014)88].

The draft Recommendation was discussed at the HC meeting on 7 November 2016. A revised draft was discussed and approved by the SPDE on 15-16 November 2016. A further revised version was discussed and approved by CDEP on 17-18 November 2016, and by the HC by written procedure on 21 November 2016.

The draft Recommendation was adopted by the OECD Council during its meeting of 13 December 2016.

The Recommendation of the OECD Council on Health Data Governance was welcomed by OECD Health Ministers on 17 January 2016 at the meeting of the HC at the Ministerial Level and it was declassified for public dissemination.

[8] 2015 OECD report *Health Data Governance: Privacy, Monitoring and Research* available at http://www.oecd.org/publications/health-data-governance-9789264244566- en.htm.