5 December 2019

RECOMMENDATION ON THE PROTECTION AND USE OF HEALTH-RELATED DATA

Mandate of the United Nations Special Rapporteur on the Right to Privacy – Task Force on Privacy and the Protection of Health-Related Data

Table of contents

Introduction

The Task Force on Privacy and the Protection of Health-Related Data was established by Professor Joseph A. Cannataci, the United Nations Special Rapporteur on the Right to Privacy (UNSRP). This recommendation was prepared under the guidance of the UNSRP and the Chairperson of MediTAS, Professor Nikolaus Forgó, and drafted by Sean McLaughlan, Secretariat to the Task Force on Privacy and the protection of health data (MediTAS). This recommendation includes the contributions of the members of MediTAS, including Teki Akuetteh Falconer, Heidi Beate Bentzen, Elizabeth Coombs, Kenneth W. Goodman, Emily Johnson, Jane Kaye, Sean McLaughlan, Trix Mulder, Katerina Polychronopoulos, Chris Puplick, Mariana A. Rissetto, William Smart, Sam Smith, Steve Steffensen, Thomas Trezise, Melania Tudorica, Marie-Catherine Wagner and Helen Wallace.

The draft document was presented and intensely discussed during the international public consultative meeting on 11 and 12 June 2019 in Strasbourg, France. More than 50 participants at that meeting contributed. In addition, the document was open for comments to the public via several communication channels. More than 30 entities/individuals provided input.

As a result, the document is the outcome of the collaboration and contribution of many participants and is not solely the work of the authors and/or of the UNSRP.

Chapter I. General provisions

1. Purpose

1.1. The purpose of this recommendation is to provide guiding principles concerning data processing of health-related data and to emphasise the importance of a legitimate basis of data processing of health-related data by all sectors of society including public authorities and commercial organisations.

1.2. This recommendation is to serve as a common international baseline for minimum data protection standards for health-related data for implementation at the domestic level, and to be a reference point for the ongoing debate on how the right to privacy can be protected in the context of health-related data, in conjunction with other human rights where health-related data is processed and shared globally.

2. Scope

2.1 This recommendation is applicable to the data processing of health-related data in all sectors of society including the public and private sectors.

2.2 This recommendation does not limit or otherwise affect any law that grants data subjects more, wider or better rights, protection, and/or remedies than this recommendation. This recommendation does not limit or otherwise affect any law that imposes obligations on processors where that law imposes higher, wider or more strict obligations, requirements, duties and/or liability than this recommendation. Where this recommendation specifies or identifies a group of people/individuals, any provisions relating to that group/individuals are in addition to any other rights, protections and/or remedies enjoyed by those people/individuals under this recommendation or any other law.

2.3 This recommendation does not apply to health-related data processing performed by individuals in the context of purely personal or household activities.

3. Definitions

For the purposes of this recommendation, the following definitions are used:

- “anonymisation” means an irreversible process applied to personal data including health-related data so that the data subject is not identifiable under any circumstances or by any means either directly or indirectly, including with the use of, or by linkage to, other data.

- “competent supervisory authority” means an independent public authority whose role, either solely or in conjunction with other purposes, is to oversee the implementation of, and compliance with, the terms of this recommendation.

- “consent” means a clear affirmative act establishing a freely given, express, explicit, specific, informed and unambiguous indication of the data subject’s agreement to the processing of personal data and/or health-related data relating to them, such as by a

written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data and/or health-related data. Silence, pre-ticked boxes or inactivity does not constitute consent. Consent should cover all data processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for each and every purpose. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

- "controller" means the natural or legal person or persons, public authority, service provider, agency or any other body which, alone or jointly with others, has the decision-making power with respect to the processing of health-related data.

- "crossborder" means across State borders, including across subnational borders internal to the State. Crossborder data transfer occurs whenever data is transferred across State borders, where data transmitted between a sender and a recipient located in the same State is sent via another State, or where one or more persons have, or may under certain conditions have, access to the data remotely from another State.

- "data portability" means that the data subject shall have the right to request the transmission of their health-related data that are retained by an automated processing system and/or hard copy file or records to another entity (including the data subject) chosen by the data subject wherever technically possible for reasonable costs, in a structured, interoperable and machine-readable format.

- "data processing" means any operation or set of operations which is performed on health-related data, such as the collection, recording, organisation, structuring, storage, sale, preservation, adaptation or alteration, retrieval, access, consultation, use, disclosure, dissemination, making available, sharing, alignment or combination, restriction, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on data, and automatic processing of health-related data.

- "data subject" means an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- "disability" is an evolving concept; disability results from the interaction between persons with impairments and attitudinal and environmental barriers that hinders their full and effective participation in society on an equal basis with others. Persons with disabilities include those who have physical, mental, intellectual or sensory impairments which in interaction with various barriers may hinder their full and effective participation in society on an equal basis with others.[1]

[1] Drawn from Convention on the rights of persons with disabilities.

- “examination” means any non-genetic or genetic test with non-clinical, diagnostic or predictive value. The results of an examination are of diagnostic value if they confirm or negate a diagnosis of a disease in a person. The results of an examination are of predictive value, if they indicate a risk of the development of a disease in the future. Examination also includes uses by law enforcement authorities (e.g. DNA screening for current or predictive investigations).

- “genetic data” means all personal data relating to the genetic characteristics of an individual which have been either inherited or acquired during prenatal development, as they result from an analysis of a biological sample from the individual concerned, in particular chromosomal, DNA or RNA analysis or analysis of any other element enabling equivalent information to be obtained. The inherited nature of DNA means that the analysis of an individual’s DNA may also have implications for other relatives, groups and populations. Genetic data includes information about the phenotype of an individual. Genetic data is health-related data under this recommendation.

- “genetic test” means tests which are carried out for analysis of biological samples of human origin and aiming specifically to identify the genetic characteristics of a person which are inherited or acquired during early prenatal development. The analysis undertaken in the context of genetic tests is carried out on chromosomes, DNA or RNA or any other element enabling equivalent information to be obtained.

- “health information system” means a system that provides the underpinnings for decision-making and has a number of functions such as: data generation, compilation, analysis, storage and synthesis, and communication and use. The health information system collects data from the health sector and other relevant sectors, analyses the data and ensures their overall quality, relevance and timeliness, and converts data into information for health-related decision-making.[2] Under this recommendation an electronic health record (EHR) is considered as a health information system.

- “health-related algorithms” means software or computer-based algorithms that help make health decisions or analyse health-related data. This includes algorithms both with and without human interference.

- “health-related data” means all personal data concerning the physical or mental health of an individual, including the provision of healthcare services, which reveals information about this individual’s past, current or future health. Genetic data is health related data in the understanding of this recommendation. Health-related data concerning but not limited to data resulting from testing, such as a prenatal diagnosis, pre-implantation diagnostics, or from the identification of genetic characteristics, whether or not regarded as the health-related data of the mother, must be protected to the same level as other health-related data.

- “health-related data breach” means the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, or prevention of lawful access to

[2] *Health Metrics Network Framework and Standards for Country Health Information Systems*, World Health Organization, January 2008.

(including unlawful lock-in practices), or sale of, health-related data transmitted, stored or otherwise processed.

- "health workers" means all people engaged in actions whose primary intent is to enhance health.[3]

- "humanitarian action" means any activity undertaken on an impartial basis to carry out assistance, relief and protection in response to a humanitarian emergency. Humanitarian action may include humanitarian assistance, humanitarian aid and protection.[4]

- "indigenous data" refers to data information or knowledge, in any format or medium, which is about, from or may affect Indigenous Peoples or people of First Nations either collectively or individually and may include the language, culture, environments or resources of Indigenous Peoples. Indigenous data includes health-related data relating to Indigenous Peoples.

- "Indigenous Data Governance" means the right of Indigenous Peoples to autonomously decide what, how and why indigenous data are collected, accessed and used. It ensures that data on or about Indigenous Peoples reflects the priorities, values, cultures, worldviews and diversity of Indigenous Peoples. This includes the principles, structures, accountability mechanisms, legal instruments and policies through which Indigenous Peoples exercise control over indigenous data.

- "Indigenous Data Sovereignty" refers to the inherent rights and interests indigenous people have in relation to the creation, collection, access, analysis, interpretation, management, dissemination, re-use and control of data relating to Indigenous Peoples.

- "insured person" refers to the individual who plans to or has entered into an insurance contract. It also applies to individuals covered by public insurance or legally mandated insurance.

- "insurer" refers to private companies, social security institutions and reinsurers.

- "international organisation" means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

- "interoperability" means the ability of different information systems to communicate and exchange data.

- "intersectionality" refers to the interconnected nature of social categorizations such as social origins, ethnicity, class, and gender as they apply to a given individual or group,

[3] *Health Workers: a Global Profile*, World Health Organization, 2006, p1.
[4] https://www.privacy-web.nl/cms/files/2017-07/handbook-data-protection-and-humanitarian-action-2-.pdf

regarded as creating overlapping and interdependent systems of discrimination or disadvantage.[5]

- “mobile applications” refers to means that are accessible in a mobile environment making it possible to communicate and manage health-related data. It includes different forms such as software, wearable connected medical and health objects and other devices that may be used for preventative, diagnostic, monitoring, treatment, recreational or wellbeing purposes.

- “open data” is data that is made available for use and sharing without restraints upon location or purpose, and which does not relate to identifiable individuals. Open data can be freely used, shared and built on by anyone, anywhere, for any purpose; be freely available in a convenient and modifiable form, and provided under terms that permit reuse and redistribution including the intermixing and interoperability with other datasets for everyone without restrictions.

- “personal data” means any information relating to an identified or identifiable natural person (“data subject”).

- “processor” means a natural or legal person, public authority, agency or any other body, alone or jointly with others, which processes data only on behalf of the controller, and on the instructions of the controller.

- “profiling” means any form of automated processing of health-related data consisting of the use of health-related data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

- “pseudonymisation” means any processing of personal data and/or health-related data in such a manner that the personal data and/or health related data can no longer be attributed to a specific data subject without the use of additional information kept separately and subject to technical and organisational measures so that personal data and/or health related data cannot be attributed or is not attributable to an identified or identifiable individual. Pseudonymised data remains personal data.

- “recommendation” means this document.

- "reference framework" means a coordinated set of rules and/or processes updated and adapted to practice and applicable to health information systems, covering the areas of interoperability and security.

- “scientific research” means creative and systematic work undertaken in order to increase the stock of knowledge and/or to devise new application of available knowledge. [6] The activity must be novel, creative, uncertain, systematic, and transferable and/or reproducible. Factors for determining whether an activity is scientific research include the role of the legal entity where the activity is carried out; the role of

[5] https://www.oxforddictionaries.com/.
[6] OECD Frascati Manual 2015 http://www.oecd.org/innovation/inno/frascati-manual.htm

the natural person(s) carrying out the activity; quality standards including use of scientific methodology and scientific publication; and adherence to research ethical norms.[7] Research within any discipline that may process health-related data, including medical and health sciences, natural sciences, engineering and technology, social sciences, humanities and fine arts, is scientific research. The scientific research may be basic research, applied research or experimental development, and policy analysis, health services and epidemiology are all examples of scientific research. Scientific research can be both publicly and privately funded and conducted, and may in some cases be conducted for profit.

- "third party" means a natural or legal person, public authority, agency or body other than the data subject, insured person, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data and/or health-related data.

Chapter II. The legal conditions for data processing of health-related data

4. Principles concerning data processing of health-related data

4.1 Data processing of health-related data must comply with the following principles:

a. health-related data must be processed in a transparent, lawful and fair manner,

b. health-related data must be collected for explicit, specific and legitimate purposes and must not be processed in a manner which is incompatible with the purposes for which it was originally collected. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should not be considered to be incompatible with the initial purposes, be subject to appropriate safeguards for the rights and freedoms of the data subject,

c. data processing of health-related data should be necessary and limited to the legitimate purpose pursued and must be carried out in accordance with section 5 of this recommendation,

d. health-related data must be collected, wherever possible, from the data subject. Where the data subject is not in a position to provide the data and such data are necessary for the purposes of the data processing of health-related data, they may be collected from other sources in accordance with section 5 of this recommendation,

e. health-related data must be adequate, relevant, accurate, up to date and limited to the purposes for which the data processing is to take place, and must be fit for the purposes of the data processing is to take place,

f. processing of health-related data must take into consideration adequate security and organisational measures. Safeguards must be in place that guarantee respect for the rights of the data subject and the security of the health-related

data. Any other guarantees may be provided for by law that safeguard respect for rights and fundamental freedoms of data subjects and their health-related data,

g. health-related data must not be stored for longer than is necessary for the purposes for which the health-related data was processed and must be carried out in particular in accordance with section 10 of this recommendation, and

h. the rights of the data subject whose health-related data are involved in any instance of data processing must be respected. This includes, but is not limited to, the rights of access to the data, information, rectification, objection, erasure, and data portability.

4.2 The legitimate purposes for processing health-related data are:

a. where there are or will be direct benefits to the data subject such as health diagnosis, care, treatment, rehabilitation and convalescence of the data subject;

b. preventive health purposes and purposes of health diagnosis, administration of care or treatment, or management of health services by health workers, subject to the conditions provided for by law;

c. reasons of public health, for example mandatory notifiable diseases, protection against health hazards, communicable disease identification and containment, environmental hazards, humanitarian action or in order to attain a high standard of quality and safety for health treatment, protection against health products and medical devices, subject to the conditions provided for by law;

d. the purpose of safeguarding the vital interests of the data subject or of another individual where consent cannot be collected from the data subject, the other individual, or both;

e. reasons relating to the obligations of controllers and to exercising the rights of the data subject regarding employment and social protection, in accordance with law or any lawful collective agreement;

f. the public interest in the accountability of the planning, funding and management of the healthcare services, management of claims for social welfare and health insurance benefits and services, subject to the conditions provided for by law;

g. processing for archiving purposes in the public interest as defined by law, for scientific or historical research purposes assessed with reference to the role of the legal entity carrying out the activity, the role of the individual(s) carrying out the activity, quality standards including use of scientific methodology and scientific publication or statistical purposes subject to the conditions defined by law in order to guarantee protection of the data subject's fundamental rights and legitimate interests (see in particular the conditions applicable to the processing of health-related data for scientific research under Chapter IX);

h. reasons essential to the recognition, exercise or defence of a legal claim in relation to the health-related data intended for data processing; and

i. reasons essential to the identification of missing persons, or the location of a missing person, where there is no reason to believe that the individual said to be missing merely wishes to avoid contact, and the circumstances of the person

being missing raises concerns for their safety and well-being, on the basis of a law which provides for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject and their relatives.

4.3 Health-related privacy principles must be considered by default (privacy by default) and incorporated into the design of information systems (privacy by design).

4.4 Compliance with all applicable principles for personal data and health-related data, including but not limited to those in this recommendation, must be regularly reviewed. The controller must carry out, before commencing data processing and at regular intervals after the data processing, a written assessment of the potential impact of the processing of data foreseen in terms of data protection, use of data and respect for privacy of the data subjects, including of the measures aimed at mitigating all risks.

4.5 Controllers and processors must take all appropriate measures to fulfil their obligations with regard to health-related data, including but not limited to those in this recommendation, and must be able to demonstrate to a competent supervisory authority that all data processing of health-related data is being or has been undertaken in accordance with all applicable obligations.

4.6 Controllers and processors who are not subject to a specific level of professional secrecy such as health workers, must ensure that all data processing of health-related data is conducted in accordance with rules of confidentiality and security measures so that there is a level of protection equivalent to that imposed on health workers.

4.7 Data processing of health-related data manifestly made public by the data subject may be undertaken unless such processing would be incompatible with the rights of the data subject under this recommendation or otherwise safeguarded in law (such as for insurance purposes). Information communicated by the data subject to their contacts on social media is not manifestly making health-related data public.

5. Lawful basis of data processing of health-related data

5.1 Data processing of health-related data is lawful if, and to the extent that, the data processing is carried out in accordance with the principles stated in section 4 of this recommendation, and one of the following applies:

a. the data subject has given their consent to that data processing, except where law precludes a data subject from consenting to the data processing. Where the requirement for consent of the data subject is not precluded by law, the data subject must be informed at the time of being asked to consent of the right to withdraw consent to the data processing at any time and be notified that any such withdrawal of consent will not affect the lawfulness of any data processing already carried out on the basis of their consent prior to any withdrawal of consent. It must be as easy for any data subject to withdraw consent as to give consent. The data subject must also be provided with understandable, clear, comprehensive information relevant to making the decision to consent or not, prior to the processing or other use of their health-related data;

b. for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;

c. for compliance with a legal obligation to which the controller is subject;

d. to protect the vital interests of the data subject or of another natural person;

e. for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or

f. for legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data and health-related data, in particular where the data subject is a child. This does not apply to processing carried out by public authorities in the performance of their tasks.

6. Notifiable Diseases and Health-Related Data

6.1 Processing of health-related data necessary for reasons of public interest in the area of public health, such as reporting of notifiable diseases, is to be undertaken in accordance with the provisions outlined in this Chapter and in Chapter III, and with ethical consideration of advising the person concerned, while providing suitable and specific measures to safeguard their rights and freedoms.

6.2 Care must be taken to ensure that the health-related data of individuals subject to a notifiable diseases report, and which identify the individual as having been subject to such a report, are given particular attention and protection so as not to subject that individual to any additional subsequent opprobrium or discrimination.

7. Genetic data

7.1 Data processing of genetic data may only be undertaken subject to appropriate safeguards and where it is either prescribed by law or on the basis of the consent expressed by the data subject in accordance with the provision of section 5(a), except where the law provides that a data subject cannot or does not need to consent to any such processing of their genetic data.

7.2 Data processing of genetic data that is undertaken for preventive, diagnostic, or treatment purposes in relation to the data subject or a member of the biological family of the data subject or for scientific research may be used for that particular purpose for data processing. It may also be used to enable persons concerned by the results of such processing of genetic data to take an informed decision without revealing to those persons concerned by the results the nature of their relationship to the data subject if that relationship is not already known to them. After such purposes have been achieved, the genetic data must be destroyed in the absence of the consent of the data subject to the retention and any subsequent use of the genetic data, unless otherwise provided for by any other necessary and proportionate law.

7.3 Existing predictive data resulting from genetic tests must not be processed for other purposes including insurance (for example, life insurance) or law enforcement purposes, except where this is specifically provided for by law. In that case, their

processing should only be authorised under appropriate and proportionate criteria defined by law, in light of the type of test used and the particular risk concerned.

7.4 The data subject is entitled to know or not know, any information relating to their genetic data, subject to the provisions of sections 11.6 and 12.5 that arise from data processing of genetic data. People must be informed, prior to any data processing, of the possibility of not being informed of the results, including of any incidental findings. An individual's wish to be kept in ignorance of a diagnosis or prognosis should be respected, except where this constitutes a serious risk to the health of others. The wish not to be informed may, in exceptional circumstances, be restricted as foreseen by law, in cases such as where a health worker has a duty to provide care or where it is in the interest of public health. The information the data subject is entitled to know under this provision does not extend to unverified research results where, in an objective assessment, providing access may be misleading.

7.5 Access to genetic data from databases that do not have a specified forensic purpose for the prevention or detection of a specific crime, or the conduct of a prosecution, must:

a. be subject to judicial oversight and specific approval by a court;

b. only be provided where it is necessary and proportionate and where adequate safeguards exist in law to protect the rights and interests of the data subject;

c. provide to all participants in the database publicly accessible information about the procedures for obtaining access to the database;

d. limit access to data strictly necessary for achieving the purpose;

e. not allow general access for national security or crime prevention purposes; and

f. not provide access to health-related or genetic data for identifying individuals with genetic propensities for criminal activity for preventive purposes.

7.6 In the context of processing genetic data for criminal law enforcement purposes, such uses must only be possible for competent authorities (for the purposes of preventing, investigating, detecting, or prosecuting criminal offences or executing criminal penalties).

7.7 Data processing of genetic data for the purpose of a judicial procedure or investigation may be undertaken only when there are no alternative or less intrusive means to establish whether there is a genetic link for the production of evidence, to prevent a real and immediate danger or for the prosecution of a specific criminal offence.

7.8 Genetic data to be used for the purpose of any judicial procedure or investigation must be collected from the data subject and not from databases or biobanks that do not have a specified forensic purpose. Only in cases where it is not possible to collect the genetic data from the data subject, access to genetic data from databases with health care and/or research purposes can be granted by a court order. The database custodian may be given the opportunity to provide reasons for objection to access to the database, on behalf of the participants.

7.9 Genetic data which are processed for the purposes of judicial proceedings, such as to determine biological kinship, should be used only to establish whether or not a genetic link between the individuals exists. Such genetic data may not be used to determine other characteristics of the data subject, nor may such data derived from that genetic data be retained beyond the necessary time period to complete the original purpose of the data processing of the genetic data. These processes may only be undertaken if data subjects have given their consent to the data processing or if it is required by judicial proceedings, specified criminal investigations, or subject to the order of a court.

7.10 Genetic data can be processed for the purpose of identification of individuals in a humanitarian crisis, mass casualty event, or to assist in the identification of missing persons, only where appropriate safeguards are provided for by law or it is manifestly in the best interests of the individual. Genetic data from the family members of a missing or deceased person may only be processed if the data subject has given their consent to that data processing. Genetic data should not be retained beyond the necessary time period to complete the original purpose of the data processing of the genetic data. Only in cases where it is not possible to collect the data from the data subject or their family, genetic data held in databases with health care and/or research purposes may be accessed for these identification purposes on the basis of a court order. Such access must only be provided where it is necessary and proportionate and where adequate safeguards exist in law to protect the rights and interests of the data subject. The procedures for obtaining access must be made publicly accessible to all participants in the database. The access must be limited to data strictly necessary for achieving the original purpose.

8. Sharing of health-related data for purposes of providing and administering health care

8.1 Where health-related data are transferred by one health worker(s) to another health worker(s), for the purposes of providing and administering health care of an individual, the data subject shall be informed before the disclosure takes place, except where this proves to be impossible due to an emergency or in accordance with section 11.4.

8.2 Health-related data can, unless appropriate safeguards are provided for by law, only be communicated to an authorised recipient or recipients who is/are subject to the rules of confidentiality incumbent upon health workers, or to equivalent rules of confidentiality.

8.3 The exchange and disclosure of health-related data between health workers must be limited to the information necessary for the co-ordination or continuity of care, prevention or medico-social and social follow-up of the individual. Health workers should be able to disclose or receive health-related data necessary to care for the patient and undertake their duties according to prior authorisation. Appropriate measures must be taken to ensure the security of all data being exchanged or disclosed.

8.4 In the exchange and disclosure of health-related data, physical, technical or administrative security measures must be adopted to guarantee the confidentiality, integrity, authenticity, accuracy, and availability of health-related data. In the event of

the failure of these measures and a health-related data breach occurs, the parties to the breach must comply with the provisions of section 13 of this recommendation.

9. Disclosure of health-related data for purposes other than providing and administering health care

9.1 Health-related data may be disclosed to recipients that are authorised and required by law to have access to and possession of the health-related data. Any such processing may only be authorised under appropriate and proportionate criteria defined by law, in light of the type of test used and the particular risk concerned.

9.2 Insurance companies, employers and contractors cannot be regarded as recipients authorised to have access to health-related data of individuals unless law provides for this with appropriate safeguards and in accordance with section 5.

10. Storage of health-related data

10.1 Health-related data must not be stored for longer than is necessary for the purposes for which the health-related data was processed. Where data processing of health-related data is for archiving purposes that are in the public interest, for scientific or historical research purposes or for statistical purposes, there must be appropriate measures in place to safeguard the rights and fundamental freedoms of the data subject and to prevent discrimination amongst families, groups and populations. For these very specific purposes, health-related data may be retained beyond the period of the initial purpose of the data processing provided it is pseudonymised or anonymised as soon as reasonably practicable without materially affecting the research, archiving activity or the statistical study. In the case of archives of information held by the State, the State shall be responsible for ensuring necessary and proportionate protections of that information to prevent health-related data breaches.

10.2 Storage of health-related data in proprietary formats that have an effect of denying access by the data subject to the health-related data may constitute a restriction on the exercise of rights of data subjects.

Chapter III. The rights of the data subject

11. Right to transparency of processing

11.1 The controller must take appropriate measures to inform the data subject of their right to fair and transparent processing of their health-related data. To ensure fair and transparent data processing of health-related data, the information provided to the data subject must include the following:

a. the identity and contact details of the controller/s and any processor/s;

b. the source of the health-related data being processed (where applicable);

c. the categories of health-related data concerned;

d. the purpose for which the health-related data are to be processed, and the legal basis for the data processing of that health-related data;

e. the length of time the health-related data will be stored for, or if that is not possible, the criteria used to determine that period;

f. the recipients or categories of recipients of the health-related data, and planned health-related data transfers to a country other than the country the health-related data is obtained in, or an international organisation (in this case health-related data may only be transferred to an international organisation that accepts it shall comply with the terms of this recommendation);

g. the possibility, if applicable, of objecting to the processing of their health-related data, in the conditions prescribed in section 12.4;

h. the conditions and the means made available to them for exercising via the controller their rights of access, of rectification and to erasure of their health-related data;

i. an indication that data processing of their health-related data may subsequently occur if such data processing is for a compatible purpose or is for archiving purposes that are in the public interest, for scientific or historical research purposes or for statistical purposes, in accordance with appropriate safeguards provided for by law and in compliance with the conditions prescribed in section 4.1.b;

j. an indication if automated decisions are being made, including profiling which is only permissible where prescribed by law and subject to appropriate safeguards, that may be made in respect of the health-related data;

k. the risks of the intended data processing and remedies available in the event of a health-related data breach;

l. how the data subject may lodge a complaint about the data processing of their health-related data and to whom such a complaint is to be made in each jurisdiction the data processing may occur in;

m. the identity and contact details of data protection officers or data controllers from whom the data subject may seek further information in relation to the proposed data processing of health-related data; and

n. proposed jurisdictions the data processing of the health-related data may involve and the rights the data subject will have comparative to these rights.

11.2 The information specified in section 11.1 must be provided prior to the data processing of the health-related data, namely health-related data collection.

11.3 The information must be intelligible and easily accessible, in plain language and suited to the circumstances to enable a full understanding of the data processing of the health-related data by the data subject. Where the data subject is physically or legally incapable of receiving the information, or of making a decision based on the information, it must be provided to the person legally representing them or the person with authority to make these decisions for the data subject. If a data subject receiving information has diminished capacity, section 14 applies.

11.4 The controller is not required to provide the information in section 11.1 where

a. the data subject already has that information;

b. health-related data is permitted not to be collected directly from the data subject;

c. the data processing of that health-related data is expressly prescribed by law, or

d. it is impossible to contact the data subject, namely the data subject cannot be found or is not reachable after reasonable efforts have been made.

In such cases the controller shall take appropriate measures to protect the data subject's rights. The controller also shall provide for general information to be accessible to all data subjects, including regarding the purpose and uses of the data, access to data by third parties, and data subjects' rights.

11.5 Where the data processing of the health-related data is for archiving purposes in the public interest; or for scientific, historical research or for statistical purposes, and it is impossible to contact the data subject as the data subject cannot be found or is not reachable after reasonable efforts have been made, the data processing of the health-related data for these purposes may be undertaken provided that the health-related data is pseudonymised or anonymised before the data processing occurs, unless otherwise provided for by law.

11.6 The controller is not required to inform the data subject where data processing of health-related data is provided for by a law that is both necessary to the purpose that it is intended to achieve and proportionate in the manner it seeks to achieve this purpose with regard to the rights and freedoms of the data subject. General information should be accessible to all data subjects, including regarding the purpose and uses of the data, access to data by third parties, and data subjects' rights.

12. Right of access to, portability, rectification, erasure, and objection to the processing of health-related data

12.1 The data subject has the right to know whether the processing of their health-related data is being conducted, and if so, to obtain - without excessive delay or expense and in an intelligible form - communication of their health-related data and to have access on the same conditions to, at least, the following information where applicable:

a. the purpose or purposes of the data processing of the health-related data;

b. the categories of health-related data concerned;

c. the recipients or the categories of recipients of the health-related data and the envisaged data transfers to a third country or countries, or an international organisation or organisations;

d. the period of data-processing of the health-related data including storage;

e. the reasoning underlying data processing of the health-related data where the results of such data processing are applied to them, including in the case of profiling, which is only permissible where prescribed by law and subject to appropriate safeguards; and

f. the methods that the controller or processor applied to anonymise, pseudonymise or minimise their health-related data.

12.2 Data subjects have the right to obtain erasure of any health-related data processed contrary to this recommendation.

12.3 Data subjects are entitled to obtain rectification of inaccurate or misleading health-related data concerning them.

12.4 If the request to rectify or erase the data is refused or if the data subject's objection is rejected, the controller must provide a reason for the refusal or rejection. The data subject must be able to have that decision reviewed before a competent supervisory authority and have access to a suitable remedy if a health-related data breach has occurred. If a health-related data breach has occurred, the controller or processor must undertake the steps provided in this recommendation relating to breach notification. The data subject may also access the remedy provisions of this recommendation, or any others available to them in their relevant jurisdiction(s).

12.5 Data subjects shall have the right not to be subject to a decision significantly affecting them based solely on an automated processing, including profiling, of their health-related data. Derogation from this prohibition is only allowed where the law provides that such a data processing of health-related data can be based on the consent of the data subject or that the processing is necessary for reasons of substantial public interest. Any such law must be proportionate to the aim pursued, respect the right to data protection and the right to privacy and provide for suitable and specific safeguards to protect the fundamental rights and freedoms of the data subject. Profiling for health purposes should meet generally accepted criteria of scientific validity, clinical validity and clinical utility and be subject to appropriate quality assurance programmes.

12.6 The data subject has the right to data portability in a timely manner.

12.7 Health workers must implement all measures to guarantee that the rights of data subjects contained in this recommendation are respected, as an element of their professional conduct and obligations.

12.8 The rights of the data subject may be subject to restrictions provided for by a law that is both necessary and proportionate in the interests of:

a. protecting State security, public safety, the economic interests of the State or the suppression of criminal offences;

b. protecting the rights and freedoms of data subjects or others.

Any such law must provide for appropriate safeguards ensuring respect for the data subject's rights.

13. Right to Remedy for Health-related data breaches

13.1 Without prejudice to any available administrative or non-judicial remedy under law, a data subject has also the right to seek an effective judicial remedy where they consider that their rights under this recommendation have been infringed as a result of the data

processing of their health-related data infringing this recommendation, or they have suffered a health-related data breach.

13.2 Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a competent supervisory authority if the data subject considers that the processing of health-related data relating to them infringes this recommendation, or they have suffered a health-related data breach.

13.3 Any person who has suffered material or non-material damage as a result of an infringement of this recommendation or health-related data breach shall have the right to seek compensation from the controller or processor for the damage suffered. Any such person shall also have the right to seek punitive damages, or to have punitive damages imposed, to the necessary extent to discourage breaches of this recommendation.

13.4 Any controller involved in processing shall be liable for the damage caused by processing which infringes this recommendation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this recommendation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

13.5 A controller or processor shall be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

14. Health-related data and diminished capacity

14.1 In relation to decisions about their health-related data, any person has the right to:

a. be presumed to have the capacity to make decisions, but in the case of children, this is subject to their evolving capacity;

b. have decisions they made restricted or otherwise interfered with to the least possible extent;

c. have established by evidence the extent to which, if at all, their decision-making capacity may have been diminished;

d. adequate and appropriate support, including access to information, for their decision-making;

e. appoint another person or entity to make decisions for them;

f. participate, to the greatest extent practicable, in decision making;

g. maintenance of their cultural and linguistic environment, and values (including any religious beliefs), except where that person has expressly indicated, through writing, words or other conduct, to the contrary; and

h. confidentiality of their health-related data about their diminished capacity.

14.2 The capacity of any person to make decisions about their health-related data may differ according to the:

a. nature and extent of any impairment affecting their capacity to make decisions;

b. type of decision to be made;

c. complexity of the decision to be made;

d. expected length of time for which the consequences of the decision may affect the individual including the possibility of the effect of any decision being able to be undone should the person regain the capacity to make such decisions and wish to revisit the decision;

e. support available from members of the person's support network; and

f. method by which decisions for the individual may be made including communal decision making.

14.3 If a person has made a decision about their health-related data in the past when they had the requisite capacity to make that decision, that decision may not be overturned by virtue of them having ceased to have capacity subsequent to the making of that decision.

14.4 A person or other entity making a decision about health-related data for a person with diminished capacity must make decisions, wherever practicable to do so and provided that it will not cause harm to or exacerbate the condition of the person with diminished capacity, that are:

a. in the best interests of the person for whom the decision is being made;

b. consistent with the dignity, proper care and protection of the person with diminished capacity;

c. least restrictive of the rights of the person with diminished capacity found in this recommendation or other applicable law;

d. consistent with the views and wishes of the person with diminished capacity, as expressed orally, in writing or by conduct or in any other way; and

e. free of a conflict of interest between the decision-maker and the interests of the person for whom a decision is being made.

14.5 Where power is exercised by another person for a person with diminished capacity, and that power is exercised in breach of the terms of this recommendation, the person making the decision that was in breach is liable for that breach to the person for whom that decision was made.

14.6 A person with diminished capacity has the same rights and obligations granted under this recommendation as any other person. The provision of decision-making powers to another person or entity in the case of diminished capacity does not obviate any other provision in this recommendation.

15. Health-related data of children

15.1 In view of children's rights and children's best interest, health-related data concerning children must be protected at least to the same level as other health-related data. Children have the same rights to privacy and data protection as adults. Wherever consent is the legal basis for the processing of health-related data of a child, the child

has the right to be informed and consideration must be given to the ability of the child to fully understand consequences of processing, and any applicable laws. Therefore, where the child is below the age to fully understand the implications of processing, such processing shall be lawful only if and to the extent that consent is given or authorised by a legally authorized representative. However, the consent of a legally authorized representative should not be necessary in the context of preventive or counselling services offered directly to a child, provided that the services are offered by a health worker or health workers acting in the best interests of the child, in circumstances where the health of the child is otherwise at risk.

15.2 Once the child has reached the age of legal majority, consent (or re-consent) to participation in research should be sought.

15.3 Children have a right to withdraw their health-related data from any health information system when they reach the age of legal majority. No information should be destroyed where to do so would be in contravention of another law that is necessary and proportionate.

Chapter IV. Health-related data and Indigenous Data Sovereignty

16. Health-related data and Indigenous Data Sovereignty

16.1 Indigenous Peoples have the right, in addition to any other rights and obligations under this recommendation, to:

a. exercise control of indigenous data. This includes the creation, collection, access, analysis, interpretation, management, security, dissemination, use, reuse, infrastructure and all other data processing of indigenous data;

b. access and co-decide on indigenous data that is contextual and disaggregated (available and accessible at individual level where authorised under this recommendation or under any law, at indigenous community and First Nations levels);

c. have indigenous data that is relevant and empowers sustainable self-determination and effective self-governance for Indigenous Peoples and First Nations;

d. have indigenous data structures that are accountable to Indigenous Peoples and First Nations;

e. have indigenous data that is protective and respects the individual and collective interests of Indigenous Peoples and First Nations,

f. decide which sets of indigenous data require active governance involving Indigenous Peoples;

g. exercise indigenous data governance and indigenous data sovereignty in respect of indigenous data and the data processing of indigenous data;

h. ensure that the physical and virtual storage and archiving of indigenous data enhances control for current and future generations of Indigenous Peoples.

Whenever possible, indigenous data shall be stored in the country or countries where the Indigenous People to whom the data relates consider their traditional land to be;

i. have indigenous data collected and coded using categories that prioritise the needs and aspirations of Indigenous Peoples as determined by them; and

j. ensure that the collection, use and interpretation of indigenous data upholds the dignity of indigenous communities, groups and individuals. Data processing of indigenous data that stigmatises or blames Indigenous Peoples can result in collective and individual harm and should be actively avoided.

16.2 Indigenous data governance enables Indigenous Peoples, representatives of Indigenous Peoples and governing bodies of Indigenous Peoples to ensure that indigenous data is accurately managed. This entails States providing indigenous data governance to Indigenous Peoples and First Nations within their territorial boundaries. Indigenous data governance provides Indigenous Peoples and First Nations with the necessary tools to identify what works, what does not and why in respect of Indigenous Peoples. Effective indigenous data governance empowers Indigenous Peoples to make, or be more involved in making, decisions to support Indigenous Peoples, communities and First Nations in the ways that meet development needs and aspirations of these communities.

Chapter V. People living with disabilities and health-related data

17. People living with disabilities and health-related data

17.1 The provisions outlined in this recommendation are to be maintained without discrimination on the basis of whether or not a person is living with a disability or disabilities.

17.2 All necessary administrative and other measures are to be taken for the management of health-related data so as to ensure enjoyment of the highest attainable standard of health for an individual, without discrimination on the basis of any disability that a person may have.

17.3 The fact that a data subject may have a disability or disabilities does not obviate any other provision in this recommendation nor does it render of no effect, any decisions made by such a person in relation to their health care or the use of their health-related data.

17.4 Health-related data concerning disabilities is not to be used to restrict the enjoyment of human rights in either health or non-health contexts unless medically indicated as established by evidence, and/or in compliance with a legal requirement.

17.5 Persons with disabilities shall not be compelled to disclose their disability status or their health-related data relating to that disability. Where accreditation or certification of the fact of disability is needed to access a benefit or service by an individual, the certification of having a disability by an authority must be sufficient to establish

entitlement. It is not lawful to require disclosure of all or part of the health-related data of that individual that relates to any assessment of disability, only the outcome may be required.

17.6 All necessary measures are to be taken to ensure that systems and procedures exist whereby health-related data reflect the person's self-defined disability status. Those responsible for the collection of health-related data relevant to individuals with a disability or disabilities, should be particularly alert to the necessity to record such changes.

17.7 Access to the health-related data of individuals with a disability or disabilities must be in accordance with the general principles of this recommendation and must be dealt with on the basis of serving the interests of the data subject. That interest must not be subordinated to the claimed interest of the State or of any institution or entity. Access to health-related data and information relating to a decision to be made about the health care or participation is scientific research of a person with a disability or disabilities must be in a form that is accessible to the person living with a disability or disabilities and be provided prior to any decision being made.

Chapter VI. Gender and health-related data

18. Gender and health-related data

18.1 All necessary administrative and other measures are to be taken for the management of health-related data so as to ensure enjoyment of the right to the highest attainable standard of health, without discrimination on the basis of gender, gender identity or expression.

18.2 The rights and obligations granted under this recommendation apply to all individuals regardless of gender, gender identity or expression. The provisions outlined in this recommendation are to be maintained without discrimination on the basis of gender, gender identity or expression.

18.3 Non-conformity to binary sex classification does not obviate any other provision in this recommendation nor does it render of no effect, any decisions made by such a person in relation to their health care or the use of their health-related data.

18.4 Health-related data concerning gender, gender identity and expression is not to be used to restrict the enjoyment of human rights in either health or non-health contexts unless medically indicated as established by evidence, and/or in compliance with a legal requirement.

18.5 Health workers are to take all necessary administrative and other measures to ensure that all persons regardless of gender, gender identity or expression, have access to quality information relevant to their health care needs including that relevant to their gender, gender identity, as well as to their own health records, and that this access is treated with confidentiality.

18.6 Gender marker categories in health-related data must be accurate and include provision for non-binary classifications.

18.7 Those responsible for the collection of health-related data relevant to individuals in a gender change transition, should be ensure that health related data and systems record such changes.

18.8 All necessary measures are to be taken to ensure that systems, procedures and data collection exist to reflect the person's self-defined gender identity. Those responsible for the collection of health-related data relevant to individuals in a gender change transition, should be particularly alert to the necessity to record such changes.

18.9 Health-related data systems for recording and processing familial relationships must reflect partner recognition, for example, as 'next of kin', regardless of gender, and gender identity or expression.

18.10 Access to the health-related data of such individuals must be in accord with the general principles of this recommendation and must be dealt with on the basis of serving the interests of the subject individual. That interest must not be subordinated to the claimed interest of the State or of the relevant institution, or any of its employees, contractors or agents.

18.11 A person or an entity making a decision concerning the health-related data of a person must do so in a way consistent with that person's gender, gender identity and expression.

Chapter VII. Intersectionality and health-related data

19. Intersectionality and health-related data

19.1 Intersectionality in the healthcare context applies to both health workers and those seeking health care. The interaction of multiple factors may put individuals in an advantageous or disadvantageous position as relates to the protection health-related data. It can mean also that individuals whether health workers or individuals seeking care, may have expectations in relation to the management of health-related data that arise from the interaction of multiple factors.

19.2 Regardless of the social group an individual is part of, every individual should be provided with the same standards in relation to their health-related data.

19.3 Intersectionality should be considered throughout all stages necessary to achieve the highest and equal protection of health-related data.

Chapter VIII. Health workers and health-related data

20. Health workers and health-related data

20.1 Health-related data may only be processed by health workers bound by the obligations of professional confidentiality or bound by similar obligations of confidentiality.

20.2 Programs of education and training for health workers who process health-related data are necessary to enable the implementation of the provisions of this recommendation.

20.3 Health workers, including those charged with the data processing of health-related data have the same obligations in the discharge of their responsibilities to all individuals.

20.4 Health workers must not discriminate against data subjects.

Chapter IX. Scientific research

21. Scientific research

21.1 The processing of health-related data for the purposes of scientific research should be subject to appropriate safeguards provided for by law, comply with the provisions of this recommendation and with any other rights and fundamental freedoms of the data subject, and be carried out for a legitimate purpose.

21.2 No individual may be required or compelled to participate in scientific research without their prior consent, except where provided for by law and subject to ethics committee approval.

21.3 Further, consent to research participation is an important research ethics instrument intended to protect human dignity and integrity. Consent to research participation is not valid as a consent for data processing during that scientific research, but it may function as a data protection safeguard. The conditions in which data processing of health-related data is conducted for scientific research must be assessed by the competent independent body (for example by an ethics committee or by an independent data custodian) which includes lay members and a legal data protection expert, prior to the commencement of the scientific research. These assessments are to be reviewed periodically by the competent supervisory authority or an ethics committee or an independent data custodian to ensure compliance with the terms of the approval, and the fact of the approval. Ethics review provides a further data protection safeguard.

21.4 Also, where consent to research participation has been given, a separate lawful basis for data processing is required under section 21.3 of this recommendation. The lawful basis for data processing in scientific research may be consent. In some cases, consent to data processing for scientific research purposes is not an option, either because consent is not practicable for that specific scientific research data processing, or the conditions for valid consent to data processing cannot be met, or because the data processing is required by law.

21.5 The need to perform data processing of health-related data for scientific research must be evaluated in light of the following:

a. purposes of the scientific research;

b. the state-of-the-art of scientific knowledge;

c. respect for ethical rules;

d. the purported benefits;

e. the constraints placed on the processing of the data;

f. the risks to the data subject;

g. the risks for group harm; and

h. as concerns the processing of genetic data, the risk to the biological family sharing some of that genetic data with the data subject and the risks of identifying non-paternity or other unexpected familial relationships.

21.6 Data processing of health-related data in a scientific research project may only be undertaken if the data subject has consented to it in accordance with the provision of section 5(a) of this recommendation, except where provided for by law. Such a law must be necessary for, and proportionate to, the aim pursued, respect the right to data protection and provide for suitable and specific safeguards to protect the rights and freedoms of the data subject. These safeguards should ensure respect for the principle of data minimisation according to section 4.1(e) of this recommendation.

21.7 The data subject must be provided, in addition to what is required by Chapter III of this recommendation (including but not limited to section 11.1), with prior, transparent and comprehensible information that is as reasonably precise as possible with regard to:

a. the nature of the envisaged scientific research, the possible choices the data subject may exercise as well as any relevant conditions governing the use of the health-related data, including possible recontact and feedback of results/findings according to the principles outlined in sections 7, 8 and 9 of this recommendation;

b. the means and capacity to extract novel forms of health-related data as well as the uncertainty pertaining to what might be extractable in the future;

c. the conditions applicable to the storage of the health-related data, including access and possible communication policies;

d. the rights and safeguards provided for by law, and specifically of the data subject's right to refuse to consent to data processing for scientific research and withdrawal of consent to take part on the scientific research in the same manner as section 5(a) of this recommendation at any time, also informing that it may not be feasible to destroy health-related data that has already been analysed and/or published before withdrawal of consent according to sections 21.10 and 21.11 of this recommendation;

e. the aims, methods, sources of funding, any possible conflicts of interest, institutional affiliations of the researcher, the anticipated benefits and potential

risks of the study and the discomfort it may entail, post-study provisions and any other relevant aspects of the study;

f. the identities of any third parties who will be given access to the data, or who may lawfully seek access to the data for other purposes and how those purposes are limited;

g. planned cross border data transfer, including the legal basis for the transfer according to section 23.1 of this recommendation; and

h. the publication that is proposed for the health-related data, and if any deposit of health-related data in scientific research repositories is envisaged.

21.8 The controller should not be obliged to provide the information directly to each data subject if the conditions laid down in section 11.4 and 11.5 or 11.6 are satisfied. However, when section 11.4 and 11.5 or 11.6 applies, the information should nevertheless be made available to data subjects in a publicly-accessible way (for example, on a website) to allow them to exercise their rights.

21.9 For scientific research, including biobanks' databases, where it is not possible to determine the specific purposes for the data processing at the time of the collection of data, data subjects should be able to express consent to data processing for certain areas of scientific research or certain parts of scientific research projects or the purpose of the biobank's database, to the extent allowed by the intended purpose, with due regard for recognised ethical standards. The areas of scientific research can be indicated using the World Health Organization's International Classification of Diseases[8]. When it becomes possible to specify the purpose further, the data subject should be informed in accordance with sections 11.1, 21.7 and 21.8 of this recommendation. Digital dynamic consent may be utilized for these purposes. This provision does not in any way reduce the requirements of consent in section 5(a) of this recommendation as they apply to scientific research.

21.10 Scientists holding health-related data will be liable for any health-related data breach in respect of the health-related data while it is in their possession or control. Complementary safeguards determined by law such as requiring explicit consent or the assessment of the competent body designated by law must be established before other scientists may acquire health-related data.

21.11 Where it is technically feasible and practicable in relation to the purposes of the scientific research, health-related data must be anonymised. Where it is not technically feasible and/or practicable to anonymise health-related data, pseudonymisation of the health-related data, with the intervention of a trusted third-party at the separation stage of the identification data, should be implemented to safeguard the rights and fundamental freedoms of the data subject. The controller cannot also function as the trusted third-party. Pseudonymisation should be applied using different keys or different methods for each different scientific research study for which the health-related data is processed, except where this would compromise the scientific validity of the scientific research. This must be done where the purposes of the scientific research can be

8 https://www.who.int/classifications/icd/en/

fulfilled by further data processing of health-related data that does not permit or no longer permits the identification of data subjects.

21.12 Where a data subject withdraws consent according to section 5(a) of this recommendation or objects to the data processing according to section 12.4 of this recommendation, health-related data about the data subject processed in the course of that scientific research must be destroyed in compliance with the wishes of the data subject unless to do so would be contrary to law. If the destruction is contrary to law, the data subject must be informed of this and of the law requiring retention of the health-related data. Where anonymisation of the data may be undertaken in a manner that does not compromise the scientific validity of the research, but ensures the data subject cannot be identified even with the use of other data sets, this may be undertaken as an alternative to destruction and the data subject should be informed accordingly. Where the data subject continues to require destruction rather than anonymisation of the health-related data, this must be complied with.

21.13 If the health-related data was analysed while a legal basis for the processing was in place, destruction of the data may not be practicable and may harm the integrity of the data set for scientific research. In such cases, provided that it is vital to achieve the results of a scientific research study conducted in the public interest or where destruction would significantly affect the scientific validity of the scientific research, the health-related data processing should be strictly limited to what is necessary to achieve these purposes, but need not be destroyed. If it is not possible to remove data from scientific research that has already taken place, information about the participant should not be used for any further scientific research.

21.14 Health-related data used for scientific research must not be published in a form that enables the data subject to be identified, except:

a. where the data subject has consented to it and that consent has not been withdrawn, or

b. where law permits such publication on the condition that this is indispensable for the presentation of scientific research findings and only to the extent that the interest in publishing the data overrides the interests and fundamental rights and freedoms of the data subject.

Where the consent of the data subject to publication of health-related data that identifies that subject is withdrawn, the controller and/or data processors must destroy or take down the health-related data where practicable. Published scientific articles need not be withdrawn if there is a clear public interest in the results of the scientific research.

Chapter X. Mobile applications, devices and systems

22. Mobile applications, devices and systems

22.1 Data collected by mobile applications, devices or systems, whether implanted in the data subject or not, is health-related data where it reveals information on the data

subject's physical or mental state, or concerns their health care. This health-related data is protected by this recommendation and, where applicable, by law.

22.2 Data subjects using mobile applications, devices or systems that involve processing of their health-related data, must be provided, in addition to what is required by Chapter III of this recommendation, with prior, transparent and comprehensible information that is as reasonably precise as possible regarding the nature and functioning of the mobile application, device or system, as well as risks, including health and security risks. All necessary information on the nature and functioning of the device, application or system must be provided in order for the data subject to be able to control both its use and the use of the data which it generates and/or transmits.

22.3 Data subjects should be able to, at any time, easily withdraw their consent to data processing in the mobile application. Data subjects should be provided with tools in the mobile application allowing them to analyse the risks involved by the data processing and the possibility at any time to disconnect from the provision of health-related data.

22.4 Any use of mobile applications must be accompanied by security measures that provide for the authentication of the person concerned, including measures such as the encryption of the transmitted health-related data, and user or patient information standards on how the health-related data that is collected will be used.

22.5 Any external hosting of health-related data produced by mobile applications must comply with security rules providing for the confidentiality, integrity, access and restitution of the data upon request of the data subject. Adherence to codes of conduct or certifications is encouraged.[9]

Chapter XI. Cross border transfer of health-related data

23. Protection is to be provided to health-related data transfers

23.1 Cross border transfer of health-related data may only take place where an appropriate level of data protection according to this recommendation and taking into account national regulations is met, or on the basis of the following provisions aimed at allowing a transfer that does not ensure such an appropriate level of protection:

a. the data subject has given explicit, specific and free consent to the transfer according to section 5(a), after being informed of the applicable law and risks arising in the absence of an appropriate safeguards level of data protection;

b. the specific interests of the data subject require it in the particular case;

c. the transfer is necessary for public interests, including scientific research and the basis for the transfer is laid down by law. The transfer must constitute a necessary and proportionate measure and be subject to appropriate safeguards; or

[9] An example of a certification is ISO/IEC 30141.

d. the transfer is necessary for prevailing legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of health-related data. The controller shall inform the supervisory authority of the transfer provided that a supervisory authority exists. The controller shall, in addition to providing the information referred to in section 11.1, inform the data subject of the transfer and of the public interest or the prevailing legitimate interests pursued. Any transfer under this section must be authorised by a necessary and proportionate law; or

e. the transfer constitutes a necessary and proportionate measure for freedom of expression.

23.2 For health-related data processed in cross border cloud computing infrastructure, platform or software, and in the absence of an obligation under international law to exercise jurisdiction, a State may only exercise jurisdiction where:

a. there is a substantial connection between the matter and the State seeking to exercise jurisdiction;

b. the State seeking to exercise jurisdiction has a legitimate interest in the matter; and

c. the exercise of jurisdiction is reasonable given the balance between the State's legitimate interests and other interests.[10,11]

Chapter XII. Electronic Health Records

24. Protecting health-related data in Electronic Health Records

24.1 All individuals have a right to privacy and the confidentiality and protection of their health-related data in electronic health record (EHR) systems, both institutional and cross-institutional, which must be rigorously managed according to data protection, ethical, professional, legal and all other applicable requirements by all health workers and any person dealing with EHR systems.

24.2 Treatment of individuals cannot be withheld by virtue of the individual not having an EHR.

24.3 The main purpose for data processing of health-related data in an EHR system is to achieve successful health treatment of patients by using and having access to better health-related data to achieve that end.

24.4 No health-related data in an EHR is to be destroyed where to do so would be in contravention of another law that is necessary and proportionate.

24.5 Mandatory information regarding disclosure and how health-related data is handled, and an ability to opt out must be provided to data subjects if not excluded by a necessary and proportionate law.

24.6 Data subject may elect to prevent disclosure of their health-related data in an EHR, documented by one health worker during treatment, to other health workers, if they choose to do so.

24.7 An EHR system must be auditable and include electronic protocol of who had access to data in an EHR, duration of that access, logs of modification and protocols to ensure unauthorised access does not occur and that data subjects know who has had access to their health-related data, duration of that access, any modification of their health-related data, and whether or not any unauthorised access has occurred. An EHR system must also be secure in line with the terms of this recommendation.

24.8 Health workers or authorised personnel of health-care institutions who process health-related data in an EHR of a data subject must:

a. be, or reasonably expect to be, treating the data subject; or

b. have the prior consent of the data subject to process the health-related data.

This section in no way limits the ability of IT personnel or other employees or contractors engaged to maintain or perform other work on the EHR itself.

24.9 There must be common standards for data accuracy and quality for all health-related data stored in an EHR.

24.10 Evidence of a patient's consent to accessing their EHR data is necessary. Reliable instruments for such proof must be provided in any EHR system. Such proof must be electronically documented for auditing purposes. The same is true for evidence of a patient's withdrawal of consent. Electronic means to give and withdraw consent have to be usable wherever technically feasible.

24.11 Where direct access by a data subject to their health-related data in an EHR is a feature of any EHR system, the operator of that EHR system must ensure that secure electronic identification and authentication is provided to prevent access by unauthorised persons.

24.12 No person shall be induced to disclose or provide access to the health-related data in their EHR where such access or disclosure is not provided for or required.

24.13 Data processing of health-related data in EHR systems for the purposes of health scientific research and statistical purposes is allowed where necessary for previously determined, specific purposes and there is a necessary and proportionate law that protects the data subject's rights.

24.14 Health-related data from EHR systems that are to be used for research purposes must be in an anonymised form wherever possible.

24.15 A data subject must have access to their health-related data in an EHR. Access must be given without undue delay or expense.

24.16 EHR systems may have many different controllers, and where there is more than one controller, a single entity must be made responsible to data subjects for the proper handling of access and other requests about the EHR.

24.17 Health-related data should not be stored in an EHR beyond the time required for the purposes for which it was collected.

24.18 Regular internal and external auditing of access protocols in any EHR must take place and be reported publicly. Entities that use EHR systems must have data protection officers to assist data subjects and health workers with meeting their obligations in respect of the EHR.

24.19 No health insurance company may be granted access to the EHR of a data subject unless provided for a necessary and proportionate law. Access should be provided using standard protocols within EHR systems and transmitted electronically to the insurance company with the prior consent of the data subject.

Chapter XIII. Health-related data and insurance

25. Health-related data and insurers

25.1 Genetic data linked to an identifiable person may not be disclosed or made accessible to insurers except where there is an important public interest provided for by domestic law, consistent with the international law of human rights or where the consent of the data subject has been obtained.

25.2 Health-related data obtained for scientific research purposes shall not be used for insurance related purposes in respect of the data subjects from which it was obtained, or the biological family members of those data subjects.

26. Insurers must justify data processing of health-related data

26.1 Health-related data may only be processed for insurance purposes subject to the following conditions:

a. the purpose of processing has been specified and the relevance of the data has been duly justified and the person has been informed about the relevance to the risk that is being insured and the justification;

b. data resulting from a predictive examination have a high positive predictive value where;

i. the quality and validity of the proposed data processing of the health-related data are in accordance with generally accepted scientific and clinical standards; and

ii. processing is duly justified in accordance with the principle of proportionality in relation to the nature and importance of the risk in question.

26.2 Health-related data from family members of the insured person should not be processed for insurance purposes, unless specifically authorised by a necessary and proportionate law. If so, the criteria laid down in section 25.1 and the restriction laid down in section 28 must be respected. The only permitted exceptions should be in cases where the information is relevant and where the family members concerned gave their consent prior to any such data processing.

26.3 The processing of publicly accessible health-related data, for example from social media or internet fora, is not permitted to evaluate risks or calculate premiums for insurance purposes. Such a breach of data protection may lead to liability as well as sanctions. The competent authorities will regulate the sanctioning regime in this respect, as well as carry out monitoring and inspection functions in this sector in accordance with section 31.3.

26.4 Questions posed by the insurer to data subjects seeking insurance should be clear, intelligible, direct, objective and precise. Insurers must provide easy and free access to a contact person that has the requisite competence and experience to address any difficulties in understanding the processing of health-related data.

27. Insurers must not process health-related data without the consent of the insured person or data subject

27.1 Health-related data must not be processed for insurance purposes without the insured person's consent in accordance with section 5(a).

27.2 Health-related data must be collected from the insured person by the insurer. The transmission of health-related data by a different entity may only be made with the consent of the insured person.

28. Insurers must have adequate safeguards for the storage of health-related data

28.1 Insurers may not store health-related data which is no longer necessary for the fulfilment of the purpose for which it was collected. Insurance companies may not store health-related data if an application for insurance has been rejected, or if the contract has expired and claims can no longer be made unless such storage is required by a law that is both necessary and proportionate.

28.2 Insurers must adopt internal regulations to protect the security and confidentiality of the insured person's health-related data. In particular, health-related data should be stored with limited access separately from other data, and health-related data kept for statistical purposes should be anonymised at the first opportunity.

28.3 Internal and external audit procedures should be put in place for adequate control of the processing of health-related data with regard to security and confidentiality.

29. Insurers must not require genetic tests for insurance purposes

29.1 Predictive genetic tests must not be carried out for insurance purposes.

29.2 Data processing of existing predictive data derived from genetic data tests may not be processed for insurance purposes unless specifically authorised by law. If such tests are authorised by law, the requisite data processing should only be allowed after independent assessment of conformity with the criteria laid down in section 26.1 by the type of test used and with regard to a particular risk to be insured.

29.3 Existing data from genetic tests of family members of the insured person may not be processed for insurance purposes relating to the insured person and must be destroyed if it comes within the purview of the insurer.

30. Insurers should take account of new scientific knowledge

30.1 Insurers must regularly update their actuarial bases in line with relevant, new scientific knowledge relating to health.

30.2 The insurer must provide relevant information and justification to any insured person regarding the calculation of the premium, any additional increase in premium or any total or partial exclusion from insurance that is based, in whole or in part, on health-related data.

31. States should ensure adequate mediation, consultation and monitoring

31.1 Mediation procedures must be established to ensure fair and objective settlement of individual disputes between insured persons and insurers concerning health-related data. Insurers should inform all insured persons about the existence of these mediation procedures.

31.2 Consultation between insurers, patient and consumer representatives, health workers and the competent authorities should be promoted to ensure a well-balanced relationship between the parties and increase transparency to consumers.

31.3 Independent monitoring of practices in the insurance sector in order to evaluate compliance with the principles laid down in this recommendation must be established and monitored by a competent and independent regulator.

Chapter XIV. Health-related data and Open Data

32. Health-related data and Open Data

32.1 Sensitive high-dimensional unit-record level data about individuals, especially but not exclusively health-related data, should not be published online or exchanged unless there is sound evidence that secure de-identification has occurred and will be robust against future re-identification.

32.2 Where health-related data is released as Open Data and a health-related data breach arises from that release, the party that processes the health-related data, and the party that releases it as Open Data (where they are not the same) shall both be liable to data subjects harmed by such release.

32.3 Liability under this recommendation is in addition to any other liability for the harm caused that may exist under the relevant laws applying to data subjects and controllers.

Chapter XV. Health-related data and automated decision making

33. Health-related data and automated decision making

33.1 The data subject shall have the right

a. not to be subject to a health-related decision based solely on automated processing, including profiling, that relates to prognosis, diagnosis or treatment, or that similarly significantly affects the data subject;

b. to have the original decision made by automated processing to be reviewed and made again by a human; and

c. to have any automated decision made in reliance, either in full or in part, on their health-related data explained to them in an easily understandable manner, by a competent person that must at least include how any automated decision-making technology works, the factors that lead to the decision that has been, is being, or will be made, and for necessary information to be provided that will justify any decision that has been, is being, or will be made.

33.2 Section 33.1 shall not apply if the automated decision:

a. is necessary for entering into, or performance of, a contract between the data subject and the controller;

b. is authorised by a law to which the controller is subject, and which also lays down appropriate measures to safeguard the data subject's rights and freedoms and legitimate interests; or

c. is based on the data subject's consent and the data subject was advised prior to giving consent that the right to have a human review and remake the decision would be lost if consent was given.

33.3 In the cases referred to in points (a) and (c) of section 33.2, the controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least to ensure that the data subject has the right to obtain human intervention in the data processing on the part of the controller, to express their point of view and to contest any decision.

Chapter XVI. AI, health-related algorithms and big data

34. AI, big data and health-related algorithmic transparency and fairness

34.1 States, when regulating health-related algorithms, should be guided by the following principles:

a. health-related algorithms should be developed and regulated in a transparent, and predictable manner;

b. health-related algorithms should meet a high and specified standard of quality and safety;

c. all health-related algorithms must be fair;

d. data subjects harmed by health-related algorithms should be able to seek compensation;

e. patient and health worker representatives should be consulted before adopting health-related algorithms;

f. health workers should make the final care or diagnostic decision and always review the outputs of health-related algorithms; and

g. health workers using health-related algorithms should inform data-subjects that a health-related algorithm is being used and of the risks associated and their rights.

34.2 Health standards will not be lowered to facilitate deployment of data processing technology, whether that be health-related algorithms, big data or AI. Forms of processing that have not yet transparently proved their efficacy shall be subject to the scientific research provisions of this recommendation.

34.3 Processes and systems must be designed and implemented to identify any potential implicit algorithmic bias. Monitoring for any adverse effects of health-related algorithms, and all forms of AI and machine learning algorithms, should be undertaken in accordance with this recommendation and any relevant laws, including characteristics protected under applicable international instruments and local laws. This provision may not be used to request, require, or record additional data on any data subject.

34.4 Where a bias is identified, steps must be taken to address this bias. Any bias must be disclosed to data subjects who may be unfairly assessed by the health-related algorithm. Health workers must take biases into consideration when using health-related algorithmic tools.

34.5 Public bodies are responsible for ensuring that no health-related algorithm, big data, or AI use breaches their obligations under any international instruments, or local laws, and to transparently monitor that outcomes uphold the rights of individuals and any minority or protected populations when making decisions or delivering care using automated means.

34.6 Data sets on populations, or subsets of populations, may affect different subgroups with disproportionate consequences, whether through their inclusion or exclusion from health systems. Compatibility with international instruments must be maintained for all.

34.7 Any decision made by a health-related algorithm or AI, should be explainable to the standards of decision making under existing commitments to the rule of law. If a health-related algorithm is not sufficiently explainable, it can only be used in support of a decision unless it is being used in pre-clinical trials or research in which case the provisions of this recommendation relating to research and experimentation apply to such use of health-related algorithms. Any health worker that relies on a non-

transparent algorithmic tool in support of a decision affecting a patient carries responsibility for the decision.

Chapter XVII. Health-related data in non-healthcare settings

35. Health-related data and immigration

35.1 All individuals must be treated according to the principles enshrined in international instruments regarding human rights and freedoms.

35.2 Where issues of health status are used as criteria in making decisions about lawful immigration and health-related data is collected for that purpose, the same conditions apply to the processing of that data as apply to similar data collected from or about, citizens of that state, both in terms of primary and secondary uses.

35.3 In the case of refugees and unauthorised arrivals, a fundamental prerequisite prior to the collection of health-related data is dignity and integrity in the process of establishing the correct personal identity of the individuals concerned.

35.4 In international law, individuals cannot be denied refugee status on the basis of their health status alone and health-related data should not be processed for any purpose intended to subvert or compromise this fundamental principle.

35.5 Health-related data should be processed to the extent necessary to facilitate health care services to authorised arrivals, non-authorised arrivals and refugees within national jurisdictions.

35.6 The sharing of health-related data between international organisations responsible for the orderly management of international migration and refugee programmes or other humanitarian services may only be undertaken on the basis that all parties involved in such data-sharing adhere to minimum standards related to health-related data management as set out in this recommendation.

36. Health-related data and individuals in the care of the state

36.1 The provisions in this section apply to both publicly and privately funded institutions. These principles apply equally in relation to individuals who are the direct responsibility of state-run or state-owned institutions and to individuals where this responsibility has been transferred by the state to the non-state sector operators.

36.2 Health-related data plays a vital role in the management of the lives of individuals who are in the care of the State and where immediate control over decisions about their own lives and health-management have been taken away from them.

36.3 Health workers, including those charged with the collection, maintenance and use of health-related data have the same obligations in the discharge of their responsibilities to such individuals as they do to any individual not in those circumstances.

36.4 Those responsible for the collection of health-related data relevant to individuals in the care of the state should be particularly alert to the necessity to identify and record instances which may suggest that there has been some violation of the bodily integrity of such individuals.

36.5 Particular care in the collection and management of their health-related data must be taken where such individuals are not able, either as a result of their age, their own medical or psychiatric condition, or because they are under the control of custodial authorities, to exercise any meaningful form of consent. This principle must be particularly considered when dealing with requests for research to be carried out on such populations, or subsets thereof.

36.6 Access to the health-related data of such individuals must be in accordance with this recommendation and must be dealt with on the basis of serving the interests of the data subject. That interest must not be subordinated to the claimed interest of the State or of the relevant institution. This requires that particular attention be given to the establishment of guidelines related to the use of such health-related data in any form of treatment, management or research where consent has not been obtained from the data subjects.

36.7 Care must be taken to ensure that when health-related data of data subjects who have been in the care of the State are made available once they cease to be in that care, that data which identifies the individual as having at some stage been in state care/custody is given particular attention to ensure the data subject is not subject to any form of opprobrium or discrimination.

36.8 Health-related data may be provided to international organisations providing humanitarian services to individuals in the care of the State if they are subject to the provisions of this recommendation.

37. Health-related data and marketing

37.1 The use of health-related data for marketing is generally incompatible with privacy obligations. Respect for the privacy and confidentiality of health-related data is incompatible with individual profiling or targeting for marketing or financial gain.

37.2 Any use of health-related data for marketing purposes should be based solely upon consent, except where the law provides that a data subject cannot consent.

37.3 Individuals should not be profiled or targeted for having sought information about illnesses or conditions that they or others may have, irrespective of whether that targeting is carried out by information providers, search engines, or online platforms (including online forums and membership websites) offering health-related communities, health intermediaries, or others.

37.4 Parties are expected to publicly describe the steps they take to avoid using health-related data and information for profiling and targeting and update such steps when it is demonstrated they fall short of the intent.

37.5 Information providers and information service providers (including websites, apps, platforms and search engines) should only facilitate profiling or marketing based on health-related data if the following conditions are met:

a. data subjects' rights to privacy and confidentiality are respected;

b. the existence and purpose of the profiling and/or marketing has been clearly communicated; and

c. consent has been given and recorded and can be withdrawn as easily as it has been given.

37.6 Information intermediaries, data brokers, or other third parties who collect, license, sell or otherwise trade in health-related data (including data containing health-related proxies or inferred health characteristics) must also respect data subjects' privacy and confidentiality. Linking health-related data to other identifiable data or using health-related characteristics to build lists of individuals with particular illnesses or conditions must only ever be done with the consent of the data subjects concerned.

37.7 Advertising platforms should not permit individual profiling or targeting based on health characteristics, or proxies for those characteristics, including via sharing, other access, transmission, or copying.

37.8 Where suspected or inferred conditions might tend to make individuals more vulnerable (for example through cognitive impairment) it is incompatible with human rights obligations to permit profiling or targeted marketing of such vulnerable people.

38. Health-related data and employers

38.1 A controller of health-related data may include an employer, and the obligations of controllers in this recommendation apply to employers that are controllers. Any health-related data breach for which an employer is liable as a controller will allow the data subject affected by the breach access to remedies available in this recommendation, and elsewhere.

38.2 An employer may process relevant health-related data relating to data subjects (such as medical certificates and other medical data) provided that they comply with the requirements of this recommendation.

38.3 An employer shall not seek health-related data from a job applicant until that person has been offered a job, except for one of the following purposes:

a. to enable the employer to make reasonable adjustments to the place of work to facilitate the employment of the individual;

b. to establish whether the applicant can carry out a function that is intrinsic to the work concerned; or

c. to monitor diversity and facilitate the employment of people living with disabilities.

38.4 Data subjects must be informed by their employer about their rights and what the purposes are for the data processing of their health-related data. Such information must be specifically communicated to data subjects when a new procedure is introduced.

38.5 Data subjects have the right to access their medical files and other health-related information from their employer to be able to verify whether it is accurate and to rectify any inaccurate or incomplete information. They must also be informed on how they may exercise their rights.

38.6 Employers must make sure that health-related of data subjects is not kept for longer than necessary. Clear retention periods must be established. These can vary in accordance with the reason for the processing of the health-related data.

38.7 All human resources staff dealing with administrative or financial procedures involving health-related data should sign a confidentiality declaration and be reminded regularly of their confidentiality obligations. Organisations should carry out a risk assessment and develop, where necessary, specific security measures on access control and management of health-related data.

Chapter XVIII. Mandatory notification of health-related data breaches

39. Mandatory data breach notification of health-related data breaches

39.1 Controllers must report any serious health-related data breach to the competent supervisory authority, data protection authority, and affected individuals not later than 72 hours from becoming aware of a health-related data breach, unless a different period is provided for by law. The report must include:

a. the nature of the health-related data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of health-related data records concerned;

b. the name and contact details of the data protection officer or other contact point where more information can be obtained;

c. the likely consequences of the health-related data breach; and

d. the measures taken or proposed to be taken by the controller to address the health-related data breach, including, where appropriate, measures to mitigate its possible adverse effects.

40. Protection of reporters of health-related data breaches

40.1 Any person who has reason to believe that a controller or other person in possession of health-related data has engaged, is engaged or proposes to engage in activity that is likely to or will result in a health-related data breach, is entitled to disclose such information to the competent supervisory authority.

40.2 Any person that makes a disclosure concerning health-related data under section 13.1 is entitled to protection whereby it is an offence to take reprisal action against the

individual for having made that disclosure concerning health-related data breaches. Such a disclosure is a protected disclosure when it is accepted by the competent supervisory authority.

40.3 Where any protected disclosure concerns the conduct of the competent supervisory authority, provision must be made for the protected disclosure to be made to another government entity or a judicial authority for investigation. Where no such provisions are made, the individual wishing to make the protected disclosure may do so publicly and may not be subject to reprisal action.

40.4 Where an individual has attempted to make a protected disclosure under the provisions of this recommendation, but it was not accepted, and the individual elects to proceed with making public the claims they wish to make, they will not enjoy any protection against potential liability under these provisions.

40.5 The above provisions do not authorise the release of health-related data. These provisions may authorise the release of information that relates to health-related data.

Chapter XIX. Security and interoperability

41. Security

41.1 Data processing of health-related data must be conducted securely. Security measures must protect human rights and fundamental freedoms and be defined and implemented to ensure that all entities conducting data processing of health-related data observe the highest standards guaranteeing the lawfulness of any data processing of health-related data.

41.2 Data security provisions provided for by law or other regulations, which may be contained in reference frameworks, may require technical and organisational measures, that must be regularly reviewed, to protect health-related data from any health-related data breach. The law must make provisions for organising and regulating procedures concerning the collection, storage and restitution of health-related data. Current examples of the security measures required by this recommendation would include the encryption of server-side health data at rest by default. Current state of the art encryption enabling quantum resistance should be considered, however the requirements for security in this recommendation will necessitate regular revision of security provisions, that may include encryption enabling quantum resistance but are not limited to this, depending on technological developments. The access provisions of this recommendation would require ensuring relevant parties have access to the decryption keys, starting from the patient in relation to their health-related data so encrypted for security purposes.

41.3 System availability, meaning the proper functioning of systems containing health-related data, must be facilitated with measures that enable the health-related data to be made accessible in a secure way and with due regard for the level of permission of authorised persons. Such system availability is to be considered in the context of

emergency situations to ensure system availability and integrity of health-related data, including access by the data subject.

41.4 Guaranteeing the integrity of any data processing of health-related data requires mechanisms to enable verification of the data processing actions carried out on the health-related data, such as any modification, deletion, copying, comparison, integration, communication and sharing of health-related data. It also requires the establishment of measures to monitor access to and use of the health-related data, ensuring that only authorised persons are able to access, use, and engage in data processing of the health-related data. Systems containing health-related data must be auditable, meaning that it must be possible to identify the user that undertook any specific action or data processing. No data processing by any person under the authority of the controller or the processor may be undertaken except on instructions from the controller, unless required by a necessary and proportionate law.

41.5 External data hosting of health-related data must ensure the security of the health-related data and comply with all principles of personal data and health-related data protection and the right to privacy. Where external data hosting or any outsourcing of the storage and use of health-related data occurs, data subjects must be informed prior to the action being taken and given time to consider if they consent to their health-related data being dealt with in this way. If they do not consent, their health-related data should be dealt with in line with the provisions of this recommendation. Note the provisions in this recommendation relating to encryption, including encryption enabling quantum resistance.

41.6 People not directly involved in the individual's health care, including employees undergoing training, who enable the operation of information systems, may have access to health-related data in an information system that is necessary to undertake their duties. Such professionals must have full regard for the confidentiality of the information and for any applicable professional secrecy as well as comply with all laws that guarantee the confidentiality and security of the health-related data as they will be liable, in conjunction with their employer or contracting party, for any consequential health-related data breach.

42. Interoperability

42.1 Interoperability must be carried out in full compliance with the principles provided for by this recommendation and that data protection safeguards be put in place when using interoperable systems.

42.2 Reference frameworks offering a technical framework that facilitates interoperability must guarantee a high level of security. The implementation, compliance and use of such reference frameworks must be audited regularly.

Chapter XX. Liability

43. Liability for health-related data breaches

43.1 Where a health-related data breach under this recommendation has occurred, and the data subject has suffered damage, the data subject should have access to a meaningful remedy.

Bibliography

BBMRI-ERIC: Making New Treatments Possible. (2016). *New Recommendation on the processing of personal health-related data* | BBMRI-ERIC: Making New Treatments Possible. [online] Available at: http://www.bbmri-eric.eu/news-events/new-recommendation-on/

Bentzen HB. In The Name Of Scientific Advancement: How To Assess What Constitutes 'Scientific Research' In The GDPR To Protect Data Subjects And Democracy. In Kużelewska E, Terzis G, Trottier D, Kloza D (eds.), sixth volume in the European Integration and Democracy Series, Intersentia Ltd (forthcoming 2020)

Bentzen HB & Svantesson DJB, Jurisdictional Challenges Related to DNA Data Processing in Transnational Clouds. In Svantesson DJB & Kloza D (eds.), Trans-Atlantic Data Privacy Relations as a Challenge for Democracy, Intersentia Ltd (2017); 241-260

Callens, S. (2010) "The EU legal framework on e-health," in Mossialos, E., Permanand, G., Baeten, R., and Hervey, T. K. (eds) Health Systems Governance in Europe: The Role of European Union Law and Policy. Cambridge: Cambridge University Press (Health Economics, Policy and Management), pp. 561–588. doi: 10.1017/CBO9780511750496.014

Cannataci, J. A., & Mifsud Bonnici, J. P., Medical data protection in Europe: new rules vs. actual trends. Strategic Alliances Between Patient Documentation and Medical Informatics, AMICE (1995); 301-321.

Cohen, GI et al., *The Legal and Ethical Concerns that Arise from Using Complex Predictive Analytics in Health Care*, July 2014, Health Affairs, 33:7

Convention on the Rights of Persons with Disabilities and its Optional Protocol (A/RES/61/106), adopted: 13 December 2006, entered into force: 3 May 2008

Council of Europe, Consultative Committee of the Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data (2018). *Draft Recommendation on the Protection of Health-Related Data*. Strasbourg

Council of Europe Committee of Ministers to the member States (2016). *Recommendation CM/Rec(2016)8of the Committee of Ministers to the member States on the processing of personal health-related data for insurance purposes, including data resulting from genetic tests*. [online] Strasbourg. Available at: http://www.quotidianosanita.it/allegati/allegato2027308.pdf

Council of Europe (2014). *Opinion on The Draft Recommendation on The Use for Insurance Purposes of Personal Health-Related Information, In Particular Information of a Genetic and Predictive Nature.* [online] Strasbourg: Council of Europe. Available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016806b2c5f

Council of Europe, Committee of Ministers (1997). *Recommendation No. R (97) 5 of the Committee of Ministers to Member States on the Protection of Medical Data*. Adopted by the Committee of Ministers on 13 February 1997 at the 584th meeting of the Ministers' Deputies

Deguara, I. (2018). *Protecting Patients' Medical Records under the GDPR*. [online] Idpc.org.mt. Available at: https://idpc.org.mt/en/articles/Pages/synapse-article.aspx

European Data Protection Supervisor - European Data Protection Supervisor. (n.d.). *Health data in the workplace - European Data Protection Supervisor - European Data Protection Supervisor*. [online] Available at: https://edps.europa.eu/data-protection/data-protection/reference-library/health-data-workplace_en. Includes source material

European Patient Forum (2016). *The new EU Regulation on the protection of personal data: what does it mean for patients?* [online] Brussels: European Patient Forum. Available at: http://www.eu-patient.eu/globalassets/policy/data-protection/data-protection-guide-for-patients-organisations.pdf

European Union Agency for Fundamental Rights (2017), *Fundamental Rights Report 2017, FRA Opinions*. Available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-fundamental-rights-report-2017-opinions_en.pdf

Forgó N, Kollek R, Arning M, Kruegel T, Petersen, I. *Ethical and Legal Requirements for Transnational Genetic Research*, Munich 2010

Forgó N, Hänold S, Schütze B. *The Principle of Purpose Limitation and Big Data*. in New Technology, Big Data and the Law. Springer Nature, Singapore Pte Ltd. . 2017. S. 17-42

Forgó N, Haidar AN, Gerhartinger H. *Security and Privacy in Sharing Patient Data*. in Coveney P, Díaz-Zuccarini V, Hunter P, Viceconti M, Hrsg., Computational Biomedicine: Modelling the Human Body. Oxford: Oxford University Press. 2014. S. 207-231

Goodman, KW. Ethics, Medicine and Information Technology: Intelligent Machines and the Transformation of Health Care. Cambridge: Cambridge University Press, 2016.

Kondylakis H, Koumakis L, Hänold S, Nwankwo I, Forgó N, Marias K et al. *Donor's support tool: Enabling informed secondary use of patient's biomaterial and personal data*. International Journal of Medical Informatics. 2017; 97:282-292

Malafosse, J and DLA Piper France LLP legal consultancy (2015). *Introductory Report for Updating Recommendation R(97) 5 of the Council of Europe on the Protection of Medical Data*. [online] Strasbourg: Council of Europe. Available at: https://rm.coe.int/introductory-report-for-updating-recommendation-r-97-5-of-the-council-/168073510c

Mantelero, A. (2017). *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*. [online] Strasbourg: Council of Europe. Available at: https://rm.coe.int/t-pd-2017-1-bigdataguidelines-en/16806f06d0

Maiam Nayri Wingara. (2018). *KEY PRINCIPLES — Maiam Nayri Wingara*. [online] Available at: https://www.maiamnayriwingara.org/key-principles

Monteiro, R. (2014). *Medical Technologies and Data Protection Issues-Food for Thought*. [online] Strasbourg: Council of Europe. Available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806945a2

OECD Frascati Manual 2015 http://www.oecd.org/innovation/inno/frascati-manual.htm

Oxford Dictionary, https://www.oxforddictionaries.com/

Price, W. Nicholson II. Regulating Black-Box Medicine, Mich. L. Rev. Volume 116, Issue 3 (2017) at p. 425

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)

Special Rapporteur on the Right to Privacy. *Annual report to the UN General Assembly,* A/73/45712 2018, Report on Big Data – Open Data at https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx

Sullivan, Hannah R., *et al.,* Are Current Tort Liability Doctrines Adequate for Addressing Injury Caused by AI?, AMA Journal of Ethics, February 2019, Volume 21, Number 2:E160-166
Svantesson, DJB, A New Jurisprudential Framework for Jurisdiction: Beyond the Harvard Draft (2015) 109 American Journal of International Law Unbound 69

Symington, A. (2004), 'Intersectionality: A Tool For Gender And Economic Justice, Facts and Issues', The Association for Women's Rights in Development (AWID)

Te Mana Raraunga - Maori Data Sovereignty Network (2018). *Principles of Māori Data Sovereignty*. [online] Te Mana Raraunga - Maori Data Sovereignty Network. Available at: https://static1.squarespace.com/static/58e9b10f9de4bb8d1fb5ebbc/t/5bda208b4ae237cd89ee16e9/1541021836126/TMR+Ma%CC%84ori+Data+Sovereignty+Principles+Oct+2018.pdf

The Nuremberg Code, 1947

The World Health Organization's International Classification of Diseases. Available at: https://www.who.int/classifications/icd/en/

United Nations, *Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (CAT),* 10 December 1984

United Nations, *Convention on the Elimination of All Forms of Discrimination against Women (CEDAW),* 18 December 1979

United Nations, *Convention on the Rights of the Child (CRC),* 20 November 1989

United Nations, *Convention on the Rights of Persons with Disabilities (CRPD)*, 20 December 2006

United Nations, *International Convention on the Elimination of All Forms of Racial Discrimination (ICERD)*, 21 December 1965.

United Nations, *International Covenant on Civil and Political Rights (ICCPR)*, 16 December 1966.

United Nations, *International Covenant on Economic, Social and Cultural Rights (ICESCR)*, 16 December 1966

United Nations, *International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (ICMW)*, 18 December 1990

United Nations, *International Convention for the Protection of All Persons from Enforced Disappearance (CPED)*, 20 December 2006

United Nations, *Universal Declaration of Human Rights*, 1948

United Nations, *United Nations Declaration on the Rights of Indigenous Peoples*, 2007

United Nations High Commissioner for Refugees*, Convention Relating to the Status of Refugees,*1951

United Nations High Commissioner for Refugees*, Protocol Relating to the Status of Refugees*, 1967

World Health Organization*, Health Metrics Network Framework and Standards for Country Health Information Systems*, January 2008

World Health Organization*, Health Workers: a Global Profile*, 2006, p.1

World Health Organization, *Ottawa charter for health promotion, 1986*

World Medical Association, *Declaration of Helsinki – ethical principles for medical research involving human subjects*, 2018