Geneva, 04 October 2019

# EXPLANATORY MEMORANDUM TO THE 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, on his mandate of the United Nations Special Rapporteur on the Right to Privacy (UNSRP). This recommendation was prepared under the guidance of the SRP 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.*

*Therefore, the document does not necessarily reflect the individual opinions of its authors and/or of the UNSRP but should rather serve as a basis for further drafting and discussion.*

*This explanatory memorandum (memorandum) should be read in conjunction with, and as a supplement to, the recommendation. This memorandum has also been prepared on the same basis and by the same individuals in the same capacities as the recommendation.*

## Background to the recommendation

Health is fundamental to everybody's life, and all of us are, at some point in our lives, patients Changes in health status can lead to significant changes in life experience, many forever, which have implications not only for individuals, but their families and wider society. Healthcare and medical research is increasingly dependent upon the use of digital data gained from individuals and populations, for prevention, diagnosis, treatment and long-term monitoring of health conditions. We all have therefore, a shared interest in our dignity and autonomy being protected by the highest standards in health-data related scenarios.

The relationship between a data subject as a patient and a healthcare professional is highly sensitive: patients are, by definition, in a vulnerable position. The situation can be distressing, dangerous and possessing lifelong consequences. The role of a healthcare professional requires accurate and complete patient information, and processes to use this information in a standardised and transparent manner.

The protection of patients (and their genetic relatives) in these moments of existential vulnerability has been subject to legal and ethical considerations and rules for millennia. Principles like medical professional confidentiality, the obligation to establish fully informed consent for treatment, proper documentation of treatment and free choice of treating physician, are the results of centuries of thought and practice on how best to protect the rights of patients.

Every medical situation produces personal data. This data is important for treatment purposes and needs to be processed following the highest legal and ethical standards. Digitalisation is

producing more and more medical data, which will be increasingly shared between healthcare professionals as they become more specialised and required to collaborate.

Data processed for health purposes is also important for many other stakeholders and for many different purposes outside the clinic. First, the patient has a legitimate interest in controlling this data and can consent to it being shared during and after treatment. Second, other stakeholders may be interested in this data, such as patients' relatives, institutions to which the patient has an obligation, for example, social security institutions, insurance companies or employers. Thirdly, there are public institutions who are responsible for providing an efficient and effective health system, that might have an interest in obtaining access to that data for research or public health purposes. The tensions between these different interests pose challenging social, legal and ethical issues.

For the purposes of this memorandum, the numbering of the original recommendation is used for referring to paragraphs that are further elaborated on in this document. Therefore, numbering may not always be sequential. Where there are additional paragraphs in this memorandum compared with the recommendation, and these paragraphs relate to specific provisions in the recommendation, those provisions of the recommendation will be specified in the explanatory memorandum paragraph.

## Chapter I. General provisions

### 1. Purpose

1.1. Provisions 1.1 and 1.2 of the recommendation set out the purpose of the recommendation. These provisions do not require full elaboration as they are informative of the nature of the document, and the intent behind it which includes establishing an international baseline. The protection of health-related data is important due to the sensitivity of that information, and also the fact that every individual will at some point have contact with the health system to generate such data. With digitisation of this and other data there are very large quantities of data being generated. It is recognised within the recommendation that contact with smart devices will also generate health-related data captured by the provisions of the recommendation.

### 2. Scope

2.1 The provisions of the recommendation are intended to apply to all data processing of health-related data. This is regardless of the entity that carries out the processing; the means applied to perform the processing, or the context of the processing including the individuals and groups involved. The intention of regulating health-related data should be to benefit humanity.

2.2 The application of the recommendation is constrained only where data subjects enjoy better rights under other applicable laws or data processors and controllers are subject to the higher standards of care or obligations than may be the case under the recommendation. The recommendation is intended to provide additional or more favourable rights and remedies for data subjects than is otherwise the case. It does not have the effect of lessening any obligations or rights or remedies that are available to data subjects. Importantly this is the case where a group of people are identified, and specific provisions of the recommendation apply to that group. These provisions are in addition to any other provisions in the recommendation including where data processors and controllers have obligations to individuals that comprise that group even where that obligation is not described as applying to that group.

2.3 The recommendation does not intend to apply to health-related data processing performed by individuals in the context of purely personal or household activities. The determination of whether activities are purely personal will depend on the circumstances of each case.

However, the recommendation does intend to apply notwithstanding that an activity may have been undertaken by an employee in their personal capacity but performed while they are acting in the course of their employment or carrying out a service that they are contracted to perform. It is important that employers and those contracting with individuals to perform services do not avoid liability where individuals perform unacceptable actions using health-related data of individuals that the employee or contractor for example, are able to access by virtue of their employment or presence in areas or access to health-related data that they have only because of this status.

## 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 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]

- “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.

[1] Drawn from Convention on the rights of persons with disabilities.
[2] *Health Metrics Network Framework and Standards for Country Health Information Systems*, World Health Organization, January 2008.

- “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 (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.

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

4 https://www.privacy-web.nl/cms/files/2017-07/handbook-data-protection-and-humanitarian-action-2-.pdf

- “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 race, class, and gender as they apply to a given individual or group, 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

[5] https://www.oxforddictionaries.com/.

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 the natural person(s) carrying out the activity; quality standards including use of scientific methodology and scientific publication; and adherence to research ethical norms. 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 principles contained in paragraphs 4.1 (a) – (h) of the recommendation. These requirements are cumulative, that is all principles must be complied with in each and every instance of the processing of health-related data. In addition, some principles require that there must also be a legitimate purpose for any processing of health-related data. Legitimate purposes are set out in paragraph 4.2 of the recommendation.

Any processing of health-related data must be lawful and fair. It must be apparent to natural persons when health-related data concerning them are processed and to what extent the health-related data are or will be processed. Additionally, health-related data may only be processed if there is a lawful basis pursuant to section 5 of the recommendation. The principle of transparency requires that any information and communication relating to the processing of health-related data be easily accessible

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

and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of health-related data concerning them which are being processed.

Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of health-related data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which health-related data are processed should be explicit, specific, legitimate and determined at the time of the collection of the health-related data.

Health-related data should be adequate, relevant, accurate, up to date and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the health-related data are stored is limited to a strict minimum. Health-related data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. To ensure that the health-related data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that health-related data which are inaccurate are rectified or deleted. Health-related data should be processed in a manner that ensures appropriate security and confidentiality of health-related data, including for preventing unauthorised access to or use of health-related data and the equipment used for the processing.

Paragraph 4.1(b) has been worded to ensure that in strictly limited and specifically defined circumstances and where there are measures in place to protect the rights of affected data subjects, health-related data may be processed even though the use may not have been clearly set out at the point of collection or included as an original purpose.

4.2 The legitimate purposes for processing health-related data required by some of the principles in paragraph 4.1 of the recommendation are contained in paragraphs 4.2 (a)-(i). Each of those paragraphs specifies a legitimate purpose for processing of health-related data. It is sufficient that one legitimate purpose is specified for the processing of health-related data where there is a requirement for a legitimate purpose, however more than one legitimate purpose may be identified.

4.3 This provision has been worded to ensure that both privacy principles and those concerning health-related data are taken into account under this provision. It is the intention of this recommendation to ensure that privacy by default and privacy by design include consideration of broader privacy principles and other rights.

4.4 This paragraph implements a requirement to review compliance with the provisions of the recommendation. The purpose is to ensure that regular reviews are conducted and should become part of oversight and governance mechanisms without becoming an administrative burden. No timeframe has been specified for the performance of these reviews. The timeframe between regular reviews should be determined with reference

to such things as the size of the organisation, the quantity of health-related data that it deals with by way of example. It is reasonable to require that all risks be mitigated while recognising that this does not mean that all risks will be reduced to nil. There will always be some risk, and where appropriate under the terms of the recommendation, liability and accountability for the risk becoming a health-related data breach is imposed.

4.5 This provision does not require that all measures to fulfil controllers' and processors' obligations with regard to health-related data be taken, and instead introduces an objective standard of "appropriate" measures to achieve the objective of protection. It is not intended that massive costs be incurred to comply with the recommendation. What is "appropriate" will depend on the circumstances of the case and what is "appropriate" in some circumstances may not be in others.

4.6 The purpose of this provision is to ensure that data controllers and processors who are not subject to a professional level of confidentiality equivalent to health workers maintain a level of protection equivalent to that imposed on health workers, in particular rules of confidentiality and security measures.

4.7 This provision allows processing of health-related data made public by the data subject and clarifies that health-related data is not made publicly available merely by being communicated to contacts on social media. This is important due to its application under the marketing provisions of this recommendation. It is significant that there is a reference to social media and contacts in this provision, however this is not intended to limit the principle to only that form of technology. This is illustrative only, what is covered is currently identified to elucidate the principle which is that communication of health-related data to the contacts or known people of the data subject is a more limited group than the public and therefore does not obviate the provisions of this agreement in respect of that health-related data so communicated.

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

5.1 These provisions contain the lawful basis for the processing of health-related data by incorporating the principles in section 4 of the recommendation and requiring that, at least, one of the provisions of this paragraph also applies to the proposed processing of health-related data. The provisions of this paragraph are not cumulative, that is, not all of these provisions must be fulfilled for processing health-related data, merely a minimum of one in addition to complying with the principles in section 4 of the recommendation in order for the processing to be lawful under the recommendation.

a. This provision allows processing of health-related data if consent from the data subject has been obtained, except where a law prohibits a data subject from consenting to the proposed data processing of the health-related data. Consent is further defined in the definitions section of the recommendation and the meaning of this term in the recommendation is discussed in greater detail in that section.

b. This provision allows data processing of health-related data for the purposes of meeting contractual obligations. Note that the principles of this recommendation apply to ensure fairness in terms of processing and recognition of rights that might not be reflected in contractual provisions.

c. This provision allows data processing to be undertaken to comply with applicable laws and contractual obligations.

d. This provision allows data processing to protect the vital interests of the data subject or of another natural person.

e. This provision allows data processing that is in the public interest or in the exercise of any official authority vested in the controller can be carried out under the recommendation.

f. This provision allows data processing of health-related data that involves the legitimate interests of a data controller or by a third party, except where these interests are overridden by the interests or fundamental rights and freedoms of the data subject. Children are identified specifically in terms of the application of these rights in accordance with the Convention of the Rights of the Child 1989 and the General Comments of the Committee on the Convention of the Rights of the Child. The need for specific and additional care where children are concerned is underscored. There is an exemption for public authorities carrying out their tasks on the basis that the process for determining the scope of law should have been part of the process resulting in that law and accounted for the rights and freedoms of affected individuals.

## 6. Notifiable Diseases and Health-Related Data

6.1 In some countries it is mandatory to inform authorities about the diagnoses of specified diseases, and which is a legal requirement upon the health workers. In many such cases, the advice to the data subject and the management of the actual fact of a notification being made, is not clearly mandated by law. The provisions of this recommendation should be construed as requiring health workers to manage the health related data involved, the provision of a notification to authorities and advising of the data subjects concerned, with due regard to both the legal requirements for notification and also, the spirit and intent of the recommendation.

6.2 The rights and freedoms of the data subject in the context of public health issues is balanced against the possible danger that notifiable diseases present to the population. The recommendation requires that consideration of the rights of individuals contained in the recommendation are accounted for under these provisions also and considered when undertaking the processing of health-related data in the context of public health and notifiable diseases. There is also a specific requirement that consideration be given to notifying the affected individual(s) in these situations. This is consonant with dignity and fairness and to ensure that people are aware of what is being done with their health-related data.

6.3 This provision intends to provide individuals subject to a notifiable diseases report, or whom are specifically identified in connection with any instance of public health emergency, with protection of their health-related data in connection with that event, and protect their privacy, safety and dignity while recognising the necessity of identification resulting from notification to relevant authorities. The taking of steps as necessary to prevent additional harm from occurring is required. The intention of this

provision is to ensure that the health-related data for notifiable diseases are processed in the framework of sections 4 and 5 of the recommendation and is not subsequently processed to the detriment of any individuals that might be identified as this can result in discrimination and other actions detrimental for the individuals concerned.

## 7. Genetic data

7.1 Genetic data is a particularly sensitive subset of health-related data as defined in the recommendation and requires specific provisions to deal with some of the challenges data processing of genetic data can present. Genetic data can be used for a very large number of purposes beyond that which it was intended to be used when it was provided. More purposes are being discovered and the challenges these developments present need to be dealt with on a principled basis. Specific and detailed provisions may cover the use of genetic data today, but principles may also cover future uses to protect the interests of data subjects in the future. The position of the recommendation is that data processing of genetic data may only be undertaken subject to appropriate safeguards and where it is either required by law or is undertaken on the basis of the consent expressed by the data subject in accordance with section 5(a) of the recommendation. There is also an allowance for laws to provide that a data subject cannot or does not need to consent to any such processing of their genetic data.

7.2 The use of genetic data is constrained under the recommendation to the purpose for which it was collected, a general provision relating to health-related data. However, due to genetic data being partially shared amongst biological relatives, genetic data about an individual also reveals information about other individuals or may do so. A concern is where diagnostic genetic testing reveals that biological relatives may be at an increased risk of a particular disease and that early treatment or preventative steps can reduce those risks. Issues become particularly clear when considering individuals being notified of such an outcome from a test in circumstances where they believe that they have no genetic relatives. Information can then be revealed to them arising from the test. The provision requires that the safety of an individual be respected in that they be informed, but that additional and ancillary data is protected and not available to them without the consent of the individual that provided the material from which the genetic data is derived. The recommendation requires the destruction of genetic data once the purpose of the data processing has been met.

7.3 This provision limits the processing of genetic data for purposes other than that for which it was collected unless there is a specific provision in law allowing for that other use. Where there is such a law, the processing is only authorised under appropriate and proportionate criteria that are clearly defined. The criteria must be both appropriate for the purpose it is undertaken for and proportionate to the risk it is intended to address. Due to the possibility of decreased trust in the health care and health research sectors, genetic data in contrast to most other health-related data is of particular interest to a wide variety of third parties for a wide variety of other uses or purposes. Data subjects must be protected against repurposing of genetic data outside the health sector, where the genetic data may be used for purposes the data subjects may object to. The requirements for genetic data must be construed more narrowly than might be the case for other types of health-related data.

7.4 The processing of genetic data can lead to findings both anticipated and not anticipated prior to the processing of that genetic data. The person to whom the test relates is entitled to decide if they wish to know about, or not know about, any results. Individuals should be informed prior to testing of potential findings and are entitled to make a decision as to whether they want to be informed about those results. Where a health-worker has a duty to provide care or where it is in the interests of public health, an individual's right not to know may be restricted. An individual's right to know does not extend to unverified research findings as these may be misleading.

7.5 Genetic data is frequently used for forensic purposes. This can include genetic data that is kept in databases that have different purposes. The provision of access to the genetic data in health-related databases should be limited due to the applicability of the purpose limitation principle and because unconstrained use of genetic data for other purposes could severely restrict the provision of genetic data to databases that do not have forensic purposes. A series of specific requirements set out the basis for access to genetic data in databases that do not have a forensic purpose or are not for specific criminal justice or law enforcement purposes. These are set out in provisions (a)-(f) which are cumulative, in that they all must be met before any such access can be granted.

a. The purpose of judicial oversight is to ensure that access is granted only where an independent body has been satisfied that it is appropriate to do so in the circumstances of the case and on terms that satisfy that body that the terms of this recommendation and any other applicable laws have been complied with.

b. See (a) above and note the addition of requirements that access be necessary for and proportionate to the subject matter of the alleged offending and where there are adequate legal safeguards to protect the rights and interests of the data subject. The use of the term "interests" is intentionally broader than a sole reference to rights and is intended to include other matters from the perspective of the data subject.

c. Information that is to be publicly available must be provided prior to individuals contributing to any such genetic database that sets out the procedures that apply for access to the genetic data for other purposes. It is critical that data subjects are aware of the criteria for access to genetic data for such purposes to ensure transparency.

d. Limiting access to data necessary to achieve the objective is critical.

e. General access to non-forensic databases containing genetic data is not allowed.

f. Access for the purposes of attempting to identify individuals that are alleged to have genetic propensities for certain criminal activities is prohibited.

7.6 Genetic data may be processed for use in criminal proceedings, investigations and law enforcement purposes, but only by competent entities and for limited purposes related to their core functions, for which there is a significant public benefit.

7.7 Data processing of genetic data for the purpose of a judicial procedure or investigation is limited to where there are no alternative or less intrusive means to establish a genetic

link in connection with proceedings, the prosecution of a specific offence or to prevent real and immediate dangers.

7.8 This provision prevents genetic databases and biobanks from becoming the first port of call when seeking genetic data of data subjects. By requiring that collection be from the data subject, the data subject will be aware that their genetic data is being sought for this purpose. This means that they can then have access to any processes and procedures available to them, including by law, to allow this. The requirement that it not be possible to collect the genetic data from the data subject is set intentionally high for this purpose. To preserve the valuable functions performed by genetic databases and biobanks and the participation of individuals in it, it is important that the genetic data within these is protected. This is also the case because of the nature of that data and the information that it contains. Even where it is not possible to collect the genetic data from the individual, a court order is still required before the genetic data in these repositories can be accessed. Additionally, a database custodian is given an opportunity to object to access on behalf of participants in that database to ensure that any court is aware of all arguments concerning access, not just those of an affected individual. This is designed to ensure that a database custodian, or similar position holder will have standing to address any Court making such decisions concerning access.

7.9 Due to the nature of genetic data and the information that can be derived from it, or that it contains, the purpose limitation needs to be maintained specifically in respect of it. This is critically so where judicial proceedings require the use of genetic data to determine biological kinship for example. It is not acceptable or desirable to obtain genetic data for one purpose connected with judicial proceedings and use it, either at the time it is obtained or later, for wider or different purposes. This includes retaining the genetic data after it has fulfilled the purpose for which it was collected. The requirement here is to destroy the genetic data once the purpose for its collection has been fulfilled.

7.10 This provision is necessary to allow for the use of genetic data in humanitarian crises. The provision is not a compulsion to provide genetic data for the purpose of identification of individuals in a humanitarian crisis, mass casualty event, or to assist in the identification of missing persons. The provision states that if it is held, genetic data may be used in the circumstances outlined if warranted and it complies with the requirements of this provision in all other respects.

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

8.1 The purpose of this provision is to limit the transfer of health-related data between health workers without the data subject being aware of it. While there is a risk of undue restriction of the transfer of data, the unrestricted ability to transfer health-related data without the knowledge of the data subject presents a greater risk. This provision does not apply where there is an emergency involving the data subject or when other provisions designed to ensure health care are able to be provided when the individual is incapacitated. This provision requires that the data subject be informed of the transfer.

8.2 The purpose of this limitation is to preserve confidentiality of health-related data where it applies. The requirement is for anyone proposing to transfer health-related data to ensure, before any transfer, that the recipient is subject to obligations of confidence concerning health-related data. The recipient must also be an authorised recipient. The principles of data protection of health-related data should apply to it in all stages of its use and transmission.

8.3 This provision contains limitations of the purposes for which health-related data may be transferred. The primary purpose for any proposed exchange of health-related data should not be for purposes other than the care of the data subject unless they are set out elsewhere in the recommendation. The concept of prior authorisation is introduced here to avoid some of the pitfalls of consent fatigue or overload. There must be a connection between the data subject, their ongoing care or treatment as outlined, and the transfer. Prior consent to necessary transfers such as those envisaged by this provision can be granted in this case. An objective standard of appropriate measures must be taken to ensure security of the data being transferred or disclosed. In the event of any breach or other issues, the appropriateness of the measures that were taken will be subject to examination.

8.4 The security of health-related data is essential for the proper operation of a health system. This is also the case when it is being transferred, as these provisions cover. This provision sets out additional requirements for the transfer of health-related data. These are purposive and technical in nature and do not require full explanation. They are objective and may need to be justified in the event of a data breach, which is outlined here and is specified in section 13 of the recommendation.

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

9.1 Laws sometimes require the disclosure of health-related data for purposes other than providing and administering health care. The other provisions of the recommendation cover disclosure for the purposes of health care. In this provision, other purposes are required to authorised by laws that are both appropriate and proportionate bearing in mind the data subject and the purpose any such law is intended to address.

9.2 Certain categories of recipients of health-related data are specifically identified as not being entitled to receive health-related data unless the law provides for it. This is because the use of health-related data by these recipients can result in severe adverse consequences for individuals. Questions of fairness arise, and the law is required to authorise such transfers specifically, and to ensure the safeguards in section 5 of this recommendation are incorporated in the law.

## 10. Storage of health-related data

10.1 This provision introduces storage limitation in respect of health-related data. Amongst the matters this provision is intended to address are risks associated with storing health-related data for periods longer than necessary to achieve the purpose for which the health-related data was acquired. The retention of health-related data that are no longer required presents many risks in that while it is held it can be accidentally lost,

unauthorised access to that data can occur, and it can be accessed and used for other purposes. In short, the circumstances in which health-related data breaches can occur are increased by the retention of health-related data. However, retention of health-related data can also be necessary and as such a limited series of other purposes is introduced in this provision to allow for this to occur but there is a requirement to protect data subjects whose health-related data is included. In addition, requirements of pseudonymisation and anonymisation are introduced to further protect such data. Additional requirements are imposed on States that control such data to recognise the potential harms such data can cause.

10.2 This provision is intended to make it clear that when health-related data is stored, it must be stored in formats that will allow data subjects to exercise their right to access that data. In the past this has been problematic where proprietary formats for storing data have been used requiring specific, and often costly, mechanisms to access it. The effect of this is to render a right of access redundant and is a breach of the recommendation. Furthermore, there will likely be issues with data portability which is provided for in this recommendation in section 12. This provision does not prevent health-related data from being encrypted. Encryption is a different concept and provided the health-related data can be de-encrypted for viewing by the data subject when requested or anyone with a lawful and legitimate purpose for doing so, does not present these issues.

## Chapter III. The rights of the data subject

### 11. Right to transparency of processing

11.1 The recommendation requires that heath related data that is being processed must be performed transparently, that is, the data subject must be aware that their data is going to be processed. Data controllers are therefore required to take appropriate measures to inform data subjects of any such data processing and of their right to fair and transparent processing. The requirement here then is not just to inform of the fact of processing, but to also inform of the purpose for the processing. The provision then outlines that the information that must be included in any notice to a data subject has to include the following but is not limited to just the specified information. So, to fully inform and comply with this provision a data controller proposing to process health-related data may need to include information that is in addition to what is specified. The information that is specified is intended to enable data subjects to be informed and to act if they wish to do so. Note that provision 11.4 provides some circumstances where the information does not need to be provided. The information to be included where applicable, is:

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

b. the source of the heath-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 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 requirement is that data subjects must be informed of data processing of their health-related data prior to that data processing taking place in order that they can meaningfully object to such processing.

11.3 The provision requires data subjects to be informed in a meaningful way. There are requirements about the nature of the information to be provided, but also the form the information is provided in. It is critical that data subjects be informed in a manner that they understand, and that the right be realistic so that they have an opportunity to understand what will be done and to do something about it should they wish. This is a question of fairness. If a data subject receiving information has diminished capacity, section 14 applies.

11.4 This provision is intended to relieve controllers from informing data subjects where to do so serves little to no purpose. The situations where controllers do not need to inform under 11.1 are limited to 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.

Even though notification is not required, data controllers must still take appropriate measures to protect the data subject's rights. This is an objective standard and is capable of review and determination by suitable bodies. The controller is also required to 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. Note that 11.4(d) requires that it is impossible to contact the data subject and is not a lesser standard. This is intentionally the case as any controller will have to establish that it is impossible to contact a data subject as opposed to being difficult or costly or some lesser standard. The purpose of these provisions is to ensure knowledge of data subjects about the uses and frequency of uses of their health-related data and while concerns about voluminous notification provisions are noted and have some basis, the purpose of these provisions is to ensure awareness.

11.5 This provision allows for processing in specified limited circumstances to be undertaken provided that 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. It must also be not possible to contact the data subject as the data subject cannot be found or is not reachable after reasonable efforts have been made. Data processing may proceed for these limited purposes providing that the health-related data is pseudonymised or anonymised before the data processing occurs, unless otherwise provided for by law.

11.6 The notification provisions are also dispensed with 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 about such processing in any event.

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

12.1 Data subjects have the right to know when their health-related data are being processed. Where it is being processed, data subjects can obtain without delay or expense and in a way that has meaning for them, specific information about the processing that must include:

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 Where health-related data has been processed contrary to the provisions of this recommendation data subjects have the right to have that data erased. This is to ensure that data subjects have a meaningful remedy where health-related data has been misused. Data subjects would be free not to exercise this right if they wish. The purpose is to create a further disincentive to processing health-related data contrary to the provisions of the recommendation.

12.3 It is important that data held about data subjects be accurate and not misleading. Data subjects should be able to meaningfully access and have data about them that is inaccurate or misleading rectified. Where there is a dispute about accuracy of information, that dispute should be recorded so that the health-related data is known to be in dispute. Disputes are covered in the following provision.

12.4 Reasons must be provided to data subjects where controllers refuse to make rectifications. These reasons can then form the basis of a dispute before a competent supervisory authority that can make findings and a decision and enforce that decision where required. Remedies will be available either under other laws or under the recommendation where a health-related data breach has occurred. It is recommended that data protection authorities monitor events in this area as it may be a useful indicator of issues that are arising commonly and may need to be regulated.

12.5 This provision relates to automated decision making that uses health-related data. Data subjects have the right not to be subject to automated decisions unless that is provided for by law that is necessary and proportionate. Any such 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. This provision is not intended to prevent machine learning, which is principally why this must relate to a decision that effects a person.

12.6 Data portability of health-related data must be undertaken in a timely and inexpensive manner. Cost has not been referred to here as data portability should be free of charge to the individual to whom the health-related data relates.

12.7 The obligation to comply with these provisions is placed on health workers. It is their duty to ensure compliance for the benefit of data subjects.

12.8 These rights of data subjects may be restricted by necessary and proportionate laws. This is necessary to ensure that there is some flexibility in the system of rights, however this is limited to only the following situations:

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 limitation of these rights by applicable laws must contain appropriate safeguards ensuring respect for the data subject's rights.

## 13. Right to Remedy for Health-related data breaches

13.1 For the purposes of the recommendation, it is essential that where there is a health-related data breach, data subjects have access to a remedy. This is the basis for the recommendation and the main mechanism by which it works. This is in addition to oversight by regulators and operates by providing individuals with the ability to seek redress for wrongs done to them through health-related data breaches. An effective judicial remedy will be one that is aimed at compensating the individual and in appropriate circumstances allowing for punitive damages to discourage engaging in future behaviour that is also a breach as well as registering disapproval of the conduct. Remedies under this recommendation are in addition to those available at law in any relevant jurisdiction. The data subject has the right to choose what remedy they seek.

13.2 This provision reflects the involvement of competent supervisory authorities with remedies for health-related data breaches. Generally, these are effective regulators and allow for other redress mechanisms to come into play and for general conduct to be considered.

13.3 A specific right of compensation is set out in this provision. It is set with reference to a harm done and is specifically in the form of compensation and punitive damages.

13.4 The respective liability for controllers and processors under the agreement are set out here. These are not the same, although both may be liable for the same breach depending on the factual setting. Processors are only liable for processing they undertake that does not comply with the recommendation specifically directed to processors. It is therefore critical to review each provision of the recommendation to ensure if an obligation is placed on a controller, a processor or both when assessing liability.

13.5 Controllers and processors can avoid liability where they can establish that they are in no way responsible for the event that caused the damage to the data subject or resulted in a health-related data breach.

## 14. Health-related data and diminished capacity

14.1 The provisions contain rights that people have concerning their health-related data specifically in circumstances where issues of capacity arise. The list of rights is cumulative, that is that they all exist. All people have 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 While there is a presumption of capacity, capacity to make decisions differs according to individuals. It is also not necessarily binary. Some decisions may be able to be made by the person, but perhaps not all. It is important to preserve the ability to make decisions to the extent possible. The provision sets out factors that relate to the capacity of any person to make decisions about their health-related and how this might 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 Where any person has made a decision, and they had full capacity to make that decision when they made it, that decision must be respected even if they no longer have the capacity to make that same decision. The purpose of this provision is to respect the decisions made by individuals and not seek to supplant those merely by a subsequent loss or diminishment of capacity and the possible appointment of another person to make decisions.

14.4 This requires that any person or entity making a decision for someone that does not have capacity to make decisions, must follow a set of principles that apply to decisions they make in this context. There are limited provisions to avoid the application of these principles, and they are where it would exacerbate or adversely affect the individual

with diminished capacity. Wherever practicable to do so, decisions made for a person with diminished capacity must be:

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 Liability for decisions made for a person with diminished capacity that are in breach of any provisions of this recommendation, not just this section, rest with the person or entity that made the decision. They are accountable to the person for whom they made the decision and representatives may be appointed to ensure that appropriate action is taken and can be referred to appropriate governing bodies or regulators.

14.6 An important principle in this section of the recommendation is that any person with diminished capacity has the same rights and obligations granted under this recommendation as any other person. Merely having decisions made by another person or entity on your behalf does not prohibit the application of the provisions of the recommendation to individuals with diminished capacity

## 15. Health-related data of children

15.1 The baseline protection level for the health-related data of children is at least the same as it is for adults. Children should be informed of what is being done with their data even where their consent is not required due to their age. This is in accordance with the Convention on the Rights of the Child 1989.

15.2 Where children reach the age of majority and can fully consent, any decisions made for them before they were able to consent independently, such as to participate in research, must be consented to again.

15.3 Data about children in health information systems can be withdrawn when children reach the age of majority. It should be for children to review decisions made on their behalf when they become independent. This right for children is tempered where there is a necessary and proportionate law preventing the withdrawal or destruction of that health-related data.

## Chapter IV. Health-related data and Indigenous Data Sovereignty

### 16. Health-related data and Indigenous Data Sovereignty

16.1 This provision provides additional rights for Indigenous Peoples under the recommendation. Indigenous Peoples and indigenous individuals enjoy all other benefits and obligations under this recommendation. It is not limited to these sections of the recommendation only. Indigenous Peoples have the right, in addition to any other rights and obligations under this recommendation, to

a. exercise control 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, 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 Issues of data governance of indigenous health-related data require particular provision in the recommendation to enable Indigenous Peoples to accurately manage data and identify uses for that data to assist them in reaching the goals that they have determined themselves for themselves. This is about respect, fairness and empowerment. 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 their development needs and aspirations.

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

### 17. People living with disabilities and health-related data

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

17.2 This provision requires all necessary administrative and other measures be taken to achieve the enjoyment of the highest attainable standard of health for an individual, without discrimination on the basis of any disability that a person may be living with. All measures necessary to achieve that goal must be taken.

17.3 Living with a disability or disabilities does not obviate any other provision in this recommendation and does not impact on any decisions made by a person in relation to their health care or the use of their health-related data.

17.4 Health-related data should not be used to perpetuate stigmas for people living with disabilities in health or non-health contexts or 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. Any such legal requirement should be necessary and proportionate and an established requirement.

17.5 Certification of the fact of disability should be sufficient to establish entitlement to any benefit or service by an individual. Requirements to disclose health-related data or other data to establish entitlement should not be required.

17.6 Health-related data must 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 and to align what is recorded with the wishes of the person.

17.7 In the case of people living with disabilities it is important that access rights to health-related data and other information people use to make decisions and/or and information relating to a decision to be made about the processing of health-related data of a person with a disability is given in a form that is accessible for the person living with a disability.

## Chapter VI. Gender and health-related data

### 18. Gender and health-related data

18.1 This provision requires all necessary administrative and other measures be taken to achieve the enjoyment of the highest attainable standard of health for an individual, without discrimination based on gender, gender identity or expression. All measures necessary to achieve this must be taken, not reasonable measures or appropriate measures, but all measures.

18.2 The provisions of the recommendation apply without discrimination based on gender, gender identity or expression.

18.3 This provision is intended to ensure that individuals who do not conform to binary sex classification cannot be excluded from the benefits of the recommendation. Their entitlement to respect for their decisions and their health-related data under the recommendation is not diminished.

18.4 Health-related data concerning gender, gender identity and expression cannot be used to prevent the application 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. Such legal requirements must be justified by evidence and be both necessary and proportionate.

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 This is an important provision to ensure that health information systems and all other recoding systems associated with health care contain the functionality to ensure that non-binary genders can be recorded in a system in line with the wishes of the individual. This information is also protected and to be treated confidentially to ensure that the individual is not subjected to discrimination.

18.7 This is also an essential provision and has wider application that just the health sector. The ability for gender to change is a necessary function for recording systems that currently have gender as a field or form of information that is collected. Where a gender change has occurred, those systems must be able to reflect those changes, and in line with the wishes of the individual, reflect those changes in past records if so desired.

18.8 This provision mandates that all necessary changes are to be taken so that systems, procedures and data collection exist to reflect a person's self-defined gender identity. This means that all changes must be taken to reflect this, not merely reasonable all appropriate changes. 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, and to give effect to them. Individuals working in this area should be trained to ensure that health-related data reflects these changes in line with the wishes of the person,

18.9 This provision is important to ensure that partner relationships are recorded for the purposes of health-related matters regardless of gender, and gender identity or expression. The purpose of this provision is to avoid situations where relationships are not recognised within the health system for important designations, such as next of kin, and some relationships are excluded based on gender and gender identity and expression.

18.10 The purpose of this provision is to cement the primacy of the individual in the context of these rights. The purpose is to limit the ability of the State to claim interests in the area that would or may result in discrimination based on gender and gender identity and expression.

18.11 The right of a person to make decisions for themselves that should be upheld and respected should not be lessened because another person that does not approve of their gender, gender identity or expression subsequently is able to make decisions for that person. As such, this requirement ensures any persons making decisions for another must do so in a way consistent with their 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 can place people in better or worse positions in terms of the protection of their health-related data. It is important to recognise this and to account for it under the recommendation. Also, individuals may have expectations around the management of their health-related data that arise from the interaction of multiple factors. A panoply of factors, such as gender, ability, age and socio-economic location, physical/mental capacity which may be attributed to individuals can interact or intersect in ways that can lead to either advantage or disadvantage for individuals. Experiences of intersectionality can mean that individuals bring to other situations such as the healthcare setting, expectations arising from these experiences and this needs to be reflected in the recommendation.

19.2 This provision records that in the context of intersectionality, every person should be provided with the same standards in relation to their health-related data.

19.3 This provision requires that issues of intersectionality should be considered throughout all stages of health-related data and treatment 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 The processing of health-related data should only be carried out by those who are subject to obligations of professional confidentiality, codes of conduct or similar privacy obligations. The purpose of this provision is to ensure that the confidentiality of health-related data is respected and preserved in the same way for all individuals.

20.2 Education and training on the confidentiality and sensitivity of health-related data must be provided for all people working with health-related data.

## Chapter IX. Scientific research

### 21. Scientific research

21.1 Scientific research plays an important function in society and the recommendation is designed to facilitate scientific research that leads to social benefits. However, scientific research needs to be carried out appropriately, and the recommendation has fundamental provisions that are designed to ensure that scientific research can be carried out for legitimate purposes and consonant with the fundamental rights and freedoms of data subjects.

21.2 Scientific research should be conducted with the knowledge and consent of research participants. No person can be compelled to participate in research without their prior consent, or without their knowledge that they are part of scientific research. This provision is in no way intended to interfere with the double-blind scientific research testing method. Awareness must relate to being informed that you are participating in research, not necessarily for example, that you are receiving a drug being tested as opposed to a placebo.

21.3 The protection of human dignity and integrity are central to scientific research. A fundamental requirement is that individuals should give prior consent to participation in research. However, there is a difference between consent to participate in research and consent to data processing during that research. These two concepts are not the same and should not be conflated. To properly function as a safeguard for data protection, consent for data processing must be obtained at appropriate times during the course of the research. The consent procedure requires the input and review of a 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. The purpose of this is to ensure that appropriate consent points are identified, and health-related data issues are considered prior to the commencement of the research. These assessments are to be reviewed periodically by a competent supervisory authority or an ethics committee or an independent data custodian to ensure compliance with the terms of the approval, and that the approval is still valid. Ethics review provides a further data protection safeguard strengthening the protection of health-related data and providing a framework to promote compliance with the recommendation.

21.4 There must be a lawful basis for the processing of health-related data for scientific research. A lawful basis is not confined to consent and is set out in the provisions of the recommendation. The lawful basis for data processing in scientific research may be consent, but it is not limited to only this lawful basis and no other. There are circumstances (examples are given in the recommendation) where consent may not apply to scientific research. This provision and 21.5 are designed to provide mechanisms where consent may not apply, however these mechanisms are subject to the fundamental principle of data subjects being informed when their health-related data is processed.

21.5 The following circumstances are set out to ensure they are taken into consideration in any data processing of health-related data that is proposed as part of scientific research. It should be noted here the factors are cumulative, that is, they all must be considered. They are:

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 Notwithstanding any other provision in the recommendation or by law, consent is required for the processing of health-related data in scientific research, except where provided for by law. The principles of data protection should be accounted for in law and in every proposal. These include data minimisation (mentioned specifically) but also include the other principles in this recommendation such as data storage minimisation.

21.7 This provision is designed to incorporate additional consent requirements that are raised by scientific research circumstances. Again, this list is cumulative in that all provisions must be met or complied with. These requirements are also in addition to general consent requirements of 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 crossborder 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 There are circumstances where a controller is not 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 met. However, when these provisions apply, the information must be made available to data subjects in a publicly accessible way (for example, on a website) to allow them to exercise their rights. The purpose of the recommendation is to provide data subjects with information that will allow them to exercise their rights, so notification directly to data subjects is preferred, but information overload is a potential issue that needs to be considered. The recommendation seeks to provide a framework within which people receive the information they need to preserve their dignity and to foster respect, without being overly burdensome.

21.9 For some scientific research such as biobanks' in particular, it is difficult to determine the specific purposes for the data processing at the time of the collection of data. In circumstances where this applies, and it must be noted that it is not possible to determine the specific purposes for data processing, not just that it is difficult or inconvenient to, data subjects are 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. This is a practical approach to a complex issue. The areas of scientific research can be indicated using the World Health Organization's International Classification of Diseases[7]. 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 and other consent forms that may be developed that are similar, may be utilized to enable ongoing communication and the obtaining of new consents when the research purposes become evident. 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 Liability for health-related data connected with scientific research and as described in this section of the recommendation, rests with the people and entities carrying out that research. This means that people undertaking research will be liable for any health-

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

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 connected with scientific research. This provision is intended to ensure that health-related data can only be broadly shared within the research community in a lawful way.

21.11 Where technically feasible and practicable for the scientific research, health-related data must be anonymised. Where anonymisation is not feasible or practicable, 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. This is to safeguard the rights and fundamental freedoms of the data subject. The controller cannot also be 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 fulfilled by further data processing of health-related data that does not permit or no longer permits the identification of data subjects. Anonymisation and pseudonymisation do not obviate the requirements in the recommendation for consent to be obtained.

21.12 Respect for decisions made by data subjects for treatment of health-related data relating to that person is a basic human rights requirement. The recommendation seeks to adhere to this in the context of scientific research. 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. Where contrary to law, the data subject must be told of the law that prevents destruction. 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 and of their right to object to anonymisation. Where the data subject continues to require destruction rather than anonymisation of the health-related data, this must be complied with. For clarity, other arrangements with the consent of the data subject are allowed but must be adequately recorded.

21.13 This provision does not deviate from the previous provisions but contains practical provisions that can allow for use and retention of health-related data that has been processed in the course of scientific research. Where 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, where 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 This provision prevents publication of health-related data used for scientific research purposes that identifies a data subject or subjects. However, there is an exception where either of the following apply:

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 Health-related data is collected by mobile applications, devices, wearables, systems, or implants is health-related data if it reveals information about the data subject's physical or mental state, or concerns health care. This health-related data is protected by this recommendation and, where applicable, by law. Technology to which this applies should be interpreted broadly and it is the collection of data that is or relates to or can be related to health-related data that the recommendation seeks to protect.

22.2 These provisions of the recommendation are driven towards providing individuals with information about how this technology will use their health-related data so that they can make an informed decision about allowing such use of their health-related data.

22.3 Easy withdrawal of consent is fundamental to the recommendation. Data subjects should be able to, at any time, easily withdraw their consent to data processing in, for example, the mobile applications, devices, wearables, systems or implants. Data subjects should be provided with tools allowing them to analyse the risks associated with the data processing and the possibility of disconnecting from the device so health-related data is no longer provided.

22.4 Any use of mobile applications, devices, wearables or systems must be accompanied by security measures that provide for the authentication of the person concerned, the encryption of the transmitted health-related data, and the highest 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, devices, wearables or systems 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 industry certification standards is encouraged.

## Chapter XI. Crossborder transfer of health-related data

### 23. Protecting health-related data transfers

23.1 Crossborder transfer of health-related data is prevented except where there is an appropriate level of data protection according to this recommendation. However, where national regulations allow it, or where at least one of the following provisions aimed at allowing a transfer where there is not an appropriate level of protection applies, transfer to other jurisdictions without protection is allowed where:

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 the public interest, including scientific research, or prevailing legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject. The controller must have assessed all the circumstances surrounding the data transfer and provided suitable safeguards with regard to the protection of health-related data. The controller shall inform the supervisory authority of the transfer if 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 describe the public interest or the prevailing legitimate interests pursued. Any transfer under this section must be authorised by a necessary and proportionate law; or

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

23.2 This provision regulates States claiming jurisdiction in crossborder transfers of health-related data. It is important for there to be a clear connection between the state and the matter in issue to claim jurisdiction. For health-related data processed in crossborder 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.

## Chapter XII. Electronic Health Records

### 24. Protecting health-related data in Electronic Health Records

24.1 Electronic health records systems (EHR) present challenges and opportunities for the protection and management of health-related data. The rights that all individuals have includes a right to privacy and the confidentiality and protection of their health-related data in EHR systems. This is true both within institutions and between institutions. EHR systems must be rigorously managed according to data protection, ethical, professional, legal and all other applicable requirements by any person dealing with EHR systems.

24.2 An important principle contained in the recommendation is that treatment of individuals cannot be withheld by virtue of the individual not having an EHR. This is aimed at reducing coercion of people into having EHRs when they do not wish to do so. It is also aimed at preserving the principle that health care should be able to be sought anonymously so that people do not put off seeking treatment for fear of repercussions or discrimination that might follow if they are identified at the point of treatment. Generally, most EHR systems require identification of individuals to match patient records with the individual being treated. Being able to seek treatment on an anonymous basis must be preserved in EHR systems. Other issues arise such as the treatment of individuals temporarily in a country with an EHR. The EHR will record that event for an indeterminate period of time in respect of the person that may have only a passing connection with that jurisdiction.

24.3 Specifying a main purpose for data processing in EHR systems is included in the recommendation to achieve successful health treatment of patients by using and having access to better health-related data to achieve that end. This is patient centred and it is the needs of the patient that should be considered first in EHR systems when it comes to the processing of health-related data.

24.4 The destruction of health-related data in an EHR is prohibited. There are exceptions within the recommendation that would require such destruction however, and these must be complied with.

24.5 Mandatory information regarding disclosure and how health-related data is processed, and an ability to withdraw from the EHR or any aspect of it must be provided to data subjects if this is not excluded by a necessary and proportionate law.

24.6 Data subjects 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 and the consequences of that choice does not have implications for their health care that a necessary and proportionate law forbids that person from exercising this choice.

24.7 Auditability is a key part of accountability and transparency in the operations of any EHR system. The recommendation requires that all EHRs 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. The purpose of this is to ensure that accurate record keeping is kept and that health-related data breaches are able to be detected investigated and form the basis of whatever appropriate outcome is required in the circumstances.

24.8 This provision requires a connection between health workers or authorised personnel of health-care institutions who process health-related data in an EHR and the data subject. The connection is clearly specified but an important rider to the requirement is that IT personnel or other employees or contractors engaged to maintain or perform work on the EHR must be able to do so. However, anyone with access to the EHR, including the exceptions, will be subject to the provisions relating to health-related data.

24.9 There must be common standards for data accuracy and quality for all health-related data stored in an EHR. There is no reason why health-related data in an EHR should not be subject to the same principles as are elsewhere in the recommendation and this is the basis on which the recommendation has been prepared.

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 must be usable wherever that is technically feasible. The recommendation does require consent often and/or requires information to be provided, and for consent to be easy to give and withdraw. Therefore health-related data in EHRs must be subject to the same principles as for other health-related data covered by this recommendation.

24.11 Security of health-related data in EHRs is critically important, and although not the same as, is closely connected with aspects of the privacy and data protection elements in the recommendation. Where security is breached and there is unauthorised access to health-related data, there will be a health-related data breach and a privacy breach. However, the converse is not necessarily the case. In cases where data subjects can access their data in EHRs, it is critical to ensure that only the individual to whom that data relates is able to use that feature to access their data. Limited other parties may access the data, however they should not use this same mechanism to access the data.

24.12 This provision is intended to limited compulsion to provide access to data in EHRs to third parties without sufficient justification.

24.13 Data processing of health-related data in EHR systems for scientific research purposes is allowed but is controlled and limited to situations where there is a necessary and proportionate law that protects the data subject's rights. This does not limit any of the other provisions of this recommendation relating to scientific research which apply equally to health-related data no matter where they are stored.

24.14 Health-related data from EHR systems that are to be used for research purposes must be in an anonymised form wherever possible. Being in an anonymised form does not

dispense with the need to seek consent which remains intact under the provisions of this recommendation.

24.15 Access to your health-related data is a fundamental principle of data protection and privacy rights. The same obligation and rationale for access applies regardless of whether the health-related data is kept in an EHR or not. Access to health-related data in an EHR must be provided under the recommendation 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 is required to be made responsible to data subjects for the proper handling of access and other requests about the EHR. The purpose of this provision is to simplify dealings for data subjects so that they only must deal with one entity in respect of their health-related data in the EHR.

24.17 This provision is the storage limitation principle for EHRs. The storage limitation principle applies to health-related data in EHRs in the same way that it applies to health-related data stored elsewhere.

24.18 Public reporting of the outcomes of these audits is required to ensure that there is public confidence in EHRs, and that issues concerning EHRs are generally known in the community.

24.19 There is a prohibition on health insurance companies being granted access to the EHR of a data subject unless such access is provided for by a necessary and proportionate law. Where access to EHRs is provided to insurance companies it should be provided using standard protocols within EHR systems and transmitted electronically to the insurance company with the prior consent of the data subject. If these provisions are not complied with there will be no access to the EHR.

## Chapter XIII. Health-related Data and Insurance

### 25. Health-related and insurers

25.1 There is a general prohibition on genetic data of a data subject being made available to insurance companies. The reason for this is that genetic data can easily be used for different purposes other than those for which it was collected and is sensitive data. Insurance performs an important social function that enables people to be able to insure against risks and to do so fairly. The exceptions are set out.

25.2 This provision ensures that there is no transfer of health-related data that was collected for scientific research purposes to insurance companies. Should this be allowed, scientific research could be prejudiced.

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

26.1 The processing of health-related data is only allowed for insurance purposes where:

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 nature of and form of 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. The intent is to ensure that actuarial bases are kept up to date and in compliance with developments in the health field of scientific research and not left as they are because it is more convenient, expedient or favourable to or for insurers to leave the bases as they are.

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 This provision is included because the risk of a health-related data breach must like with the party that is to release health-related data, and also where the party proposing release and the party that release the data are not the same, both shall be liable to data subjects harmed by the release.

32.2 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 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 The regulation of health-related algorithms is important for several reasons, not the least of which is to ensure that the benefits they might bring are realised for the benefit of humanity. However, a potential pitfall is that there is potential for algorithmic bias and the safety of people that are exposed to early forms of technology should have to take unnecessary and ill-informed decisions concerning risk. While there are many benefits, introducing additional potential discrimination is where States should regulate to avoid that outcome. 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 A key consideration is to ensure that for the implementation of new and innovative technology, standards of health care are not lowered to facilitate the introduction of the new technology. The recommendation prohibits this and requires that new technology must have transparently proved its effectiveness before it is deployed.

34.3 Monitoring for algorithmic bias is required under the recommendation. This is to ensure that there is no bias in the algorithm and that it is performing as it should. In the absence of being monitored there can be no assurance of the absence of bias or of effective operation.

34.4 It is a requirement that identified biases be addressed. This must be done so fairly and without detriment or discrimination itself. For instance, it is not a sufficient response to address bias by excluding a group that suffered bias from the use of the algorithm. While that may be enough for a short period while the bias is rectified, it cannot be permanent.

34.5 This monitoring must be overseen or regulated by public bodies in the jurisdiction to ensure that it is performed fairly and accurately with sanctions if it is not. The exact

regulator can be decided by States, but competent supervisory authorities might be appropriate.

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. This is also the case for the data processing of health-related data in immigration contexts.

35.2 There should, as a matter of principle, be no difference between the use of health-related data for citizens than for the health-related data of people trying to migrate to a country. This is the case for both matters of privacy and for secondary uses. While disclosure of some health-related data may be required, it should be limited to only that required to carry out the proper purpose, and also in accordance with a necessary and proportionate law setting out what health-related data is required as well as to whom it, or the results of it, must be disclosed.

35.3 In the case of refugees and unauthorised arrivals, a fundamental prerequisite prior to the collection of health-related data is ensuring 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 based on 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 at least 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 manifestation of being in the care of the state is not universal. For the purposes of the recommendation it does not refer to the source of funding for an institution, but rather refers to individuals being placed in a setting where the authority that they have over themselves is diminished due to the intervention of the State actor. This can include all responsibility for making decisions that affect them being removed. For the purposes of the recommendation, this applies where the ability to make decisions about individual healthcare and\or health-related data are removed and are made by a different entity, usually the State. Examples are prisoners, people in custodial care or in immigration detention but it is not limited to these examples. In all such circumstances particular care is required. The purpose of this provision in particular is to ensure that the funding source of an institution that has individuals to whom this section may apply, is not determinative.

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 There is no reason why health workers should have less of a duty to individuals in the care of the State than they do to other individuals not in the care of the State in respect of health-related data.

36.4 In fact, there are some additional duties that health-workers might have in respect of individuals in the care of the State, such as a duty to be particularly vigilant in respect of any evidence that might suggest any violations of the bodily integrity of such individuals.

36.5 This provision builds on the idea that there are additional duties for health-care workers when dealing with individuals in the care of the State.

36.6 Access to the health-related data of individuals in the care of the State must be in accordance with this recommendation and be in the interests of the data subject. That interest must not be subordinated to the claimed interest of the State or of the relevant institution. The use of health-related data of these individuals must be carefully controlled.

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, such data is controlled and managed in accordance with the recommendations. Care must be taken to avoid disclosing health-related data that will subject the individual to opprobrium or discrimination by revealing that the person was in the care of the State.

36.8 Health-related data may be provided to international organisations providing humanitarian services to individuals in the care of the State if those international organisations 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. Without consent, an individual should not be marketed to on the basis of their health-related data or status.

37.3 Individuals should not be profiled or targeted for having sought information about illnesses or conditions that they or others may have, nor where they have undergone particular treatment. The method of targeting is not material, the targeting is prohibited.

37.4 The purpose of publicising this data is to ensure that the public are aware, and have the opportunity to make themselves aware, of best practises in the area and assess performance of various participants in this area. This is also intended to be a disincentive to any type of incompatible behaviour.

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, 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 Employers collected health-related data about their employees. Health-related data can include information about sick leave or insurance claims where health insurance

involves the employer, or about work-related accidents affecting employees. As such, employers are data controllers under the recommendation and the provisions of this recommendation apply to all controllers, including employers.

38.2 Employers need to be able to process health-related data in the course of employing staff. The recommendation permits processing by employers, but they are subject to the same obligations as other processors of health-related data under the 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, the purposes of the data processing of their health-related data, and information and details about who is being provided access to such 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 otherwise 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 The protection of reporters of health-related data breaches is important to ensure that behaviour in contravention of the recommendation can be reported and acted upon. Some of the largest revelations about dealing with personal information have come from individuals disclosing practices that were not known about. The recommendation therefore provides an avenue for reporters to come forward about any practises that they wish to concerning health-related data. Disclosures cannot be made to anyone, disclosures must be made to the competent supervisory authority.

40.2 Any person that makes a disclosure concerning health-related data under section 40.1 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. No protection is provided unless the disclosure is accepted as a protected disclosure.

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 subjected to reprisal action.

40.4 This provision provides that where an individual elects to proceed with publicising the information even if the protected disclosure has not been accepted, that individual I subject to normal action under the law.

40.5 Health-related data cannot be released or disclosed in reliance on the sections of this provision. The information that may be released relates only to information concerning what is done with the health-related data.

## Chapter XIX. Security and interoperability

### 41. Security

41.1 Data security and privacy are related concepts but are not the same. Security breaches may result in data or privacy breaches, but there is more to privacy and data protection

than security. However, security is a cornerstone of the recommendation and provisions requiring security in respect of data processing are set out in this section of the document. processing of health-related data must be conducted securely. Fundamental rights and freedoms are affected by the security of such data processing.

41.2 All laws must make relevant provision for security and for the protection of health-related data.

41.3 System availability is critical to the functioning of a health system. System outages can severely impinge the effectiveness of the health system and also be a breach of the access provisions of this recommendation. Furthermore, emergency situations are likely to impact a health system, so proper testing of health information systems and EHRs and the like are required.

41.4 These are technical provisions that outline the requirements for systems in plain language. It is up to respective jurisdictions to implement them.

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.

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.