United Nations A/74/277

General Assembly

Distr.: General
5 August 2019

Original: English

Seventy-fourth session
Item 72 (b) of the provisional agenda*
Promotion and protection of human rights: human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms

Right to privacy

Note by the Secretary-General

The Secretary-General has the honour to transmit to the General Assembly the report prepared by the Special Rapporteur on the right to privacy, Joseph A. Cannataci, submitted in accordance with Human Rights Council resolution 28/16.

* A/74/150.

19-13343 (E) 280819

Report of the Special Rapporteur on the right to privacy

Summary

The present report has been prepared by the Special Rapporteur on the right to privacy, Joseph A. Cannataci, and is submitted in accordance with Human Rights Council resolution 28/16.

The report contains a summary of activities and a recommendation on the protection and use of health-related data.

I. Summary of activities

1. Since October 2018, the Special Rapporteur on the right to privacy has visited Germany, Argentina and the Republic of Korea, on which he will report to the Human Rights Council in 2020. Work on surveillance has proceeded, inter alia, with the International Intelligence Oversight Forum, held in Malta in 2018 and to be held in London in 2019. The Special Rapporteur thanks the host Governments for supporting these events, which led to the development of a principle that must be applied to the international exchange of intelligence data: "if it's transferable, then it's oversightable". The Special Rapporteur has prepared a draft report on gender, which will be submitted to a consultation in New York on 30 and 31 October 2019, and guidelines on privacy and on children and privacy metrics. He has also developed the recommendation contained in the annex to the present report. The Special Rapporteur thanks the Council of Europe for co-hosting the consultation meeting on health-related data in June 2019.

II. Health-related data

2. The right of everyone to the enjoyment of the highest attainable standard of physical and mental health has been recognized in the Universal Declaration of Human Rights (art. 25) and in international human rights instruments such as the International Covenant on Economic, Social and Cultural Rights (art. 12), the Convention on the Rights of the Child (art. 24), the Convention on the Elimination of All Forms of Discrimination against Women (art. 12) and the Convention on the Rights of Persons with Disabilities (art. 25).

3. There is increasing awareness on the sensitive nature of health-related data. In the digital era, such data are captured and used in a myriad of ways, frequently without the concerned individual's consent or awareness. The industry of collecting and using health-related data and the growing number of data breaches are of enormous concern.

4. It was against this background that the Special Rapporteur established the Task Force on Privacy and the Protection of Health-Related Data in 2017 to prepare a recommendation on the protection and use of health-related data for Member States to use as an international baseline of minimum data protection standards for health-related data. It incorporates the results of global consultations and several hundred comments from stakeholders.

5. The recommendation was drafted under the coordination of the Secretary of the Task Force, Sean McLaughlan, guided by the Chair, Nikolaus Forgó, and with contributions from the members of the Task Force, Teki Akuetteh Falconer, Heidi Beate Bentzen, Elizabeth Coombs, Kenneth W. Goodman, Trix Mulder, Katerina Polychronopoulos, Chris Puplick, Mariana A. Rissetto, William Smart, Sam Smith, Jane Kaye, Steve Steffensen, Thomas Trezise, Melania Tudorica, Marie-Catherine Wagner and Helen Wallace.

6. The foundations of the recommendation are that everyone has the right to the highest attainable standard of physical and mental health and to the highest attainable standard of protection for their health-related data, irrespective of disability, gender, gender identity, gender expression or other factors. Consent is emphasized to protect human dignity and integrity, while provision is made for uses of health-related data that are in the public interest (such as scientific research), with appropriate safeguards.

7. Contained in the annex is an abbreviated version of the recommendation, focusing on key elements. When transposing it into domestic law, States should use the full version, which is available at www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/DraftRecommendationProtectionUseHealthRelatedData.pdf.

Annex

Recommendation on the protection and use of health-related data

Chapter I

General provisions

1. Purpose

1.1 The purpose of this recommendation is to provide guiding principles concerning data processing of health-related data.

1.2 The guidance is to serve as an international baseline for minimum data protection standards for health-related data.

2. Scope

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

2.2 It does not limit or otherwise affect any law that grants data subjects more, wider or better rights, protection and/or remedies than this recommendation.

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

3. Definitions

- "Anonymization" means an irreversible process applied to personal 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, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to her or him, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting a website, choosing technical settings for information society services or another statement or conduct that clearly indicates in this context the data subject's acceptance of the proposed processing of her or his personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for each one. 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 that, alone or jointly with others, has the decision-making power with respect to the processing of health-related data.
- "Data processing" means any operation or set of operations that is performed on personal data, such as the collection, recording, organization, structuring,

storage, sale, preservation, adaptation or alteration, retrieval, access, consultation, use, disclosure, dissemination, making available, sharing, alignment or combination, restriction, erasure or destruction of data, or the carrying out of logical and/or arithmetical operations on personal 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 that, in interaction with various barriers, may hinder their full and effective participation in society on an equal basis with others.
- "Examination" includes 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. The reliability of the results of examinations with predictive value is extremely variable. Examination also includes uses by law enforcement authorities (for example, DNA screening for current or predictive investigations).
- "Genetic data" means all personal data relating to the genetic characteristics of an individual that 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. It includes information about the phenotype of an individual.
- "Genetic test" means tests that are carried out for analysis of biological samples of human origin and aiming specifically to identify the genetic characteristics of a person that 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.[1]

[1] World Health Organization, *Framework and Standards for Country Health Information Systems*, 2nd ed. (2008).

- “Health-related data” means all personal data concerning the physical or mental health of an individual, including the provision of health-care services, that reveal information about the individual’s past, current and future health. Genetic data are 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, unauthorized 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; this does not include intentional lawful destruction.
- “Health workers” means all people engaged in actions whose primary intent is to enhance health.
- “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.[2]
- “Indigenous data” means data, information or knowledge, in any format or medium, that is about, from or may affect indigenous peoples or people of first nations either collectively or individually and may include the language, culture, genetic data, environments or resources of indigenous peoples.
- “Indigenous data sovereignty” means the inherent rights and interests that indigenous people have in relation to the creation, collection, access, analysis, interpretation, management, dissemination, re-use and control of 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 reflect 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.
- “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 organization” means an organization and its subordinate bodies governed by public international law, or any other body that 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” means the interconnected nature of social categorizations such as race, class and gender as they apply to a given individual or group,

[2] Christopher Kuner and Massimo Marelli, eds., *Handbook on Data Protection in Humanitarian Action* (International Committee of the Red Cross, 2017).

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

- “Medical algorithms” means software or computer-based algorithms that are used to help to make health decisions or analyse health information. They include algorithms both with and without human interference.
- “Mobile applications” refers to means accessible in a mobile environment that make it possible to communicate and manage health-related data. They include different forms such as software, wearable connected medical and health objects and devices that may be used for preventive, diagnostic, monitoring, treatment, recreational or well-being purposes.
- “Open data” means data that are made available for use and sharing without restraints upon location or purpose and which do not relate to identifiable individuals. Open data can be freely used, shared and built on by anyone, anywhere, for any purpose; they can be freely available in a convenient and modifiable form and provided under terms that permit reuse and redistribution, including 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, that processes data only on behalf of the controller, and on the instructions of the controller.
- “Profile” means a set of health-related data characterizing a category of individuals that is intended to be applied to an individual.
- “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.
- “Pseudonymization” means any processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information kept separately and subject to technical and organizational measures so that personal data cannot be attributed or attributable to an identified or identifiable individual. Pseudonymized 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 to increase the stock of knowledge and/or to devise new applications of available knowledge. The activity must be novel, creative, uncertain, systematic, transferable and/or reproducible. Factors for determining whether an activity constitutes 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. Policy analysis, health services and epidemiology are all examples of scientific research. Scientific research can be publicly and/or privately funded and conducted, and may in some cases be conducted for profit.

- "Transborder" means across State borders, including across subnational borders that are internal to the State. Transborder data transfer occurs whenever data are transferred across State borders, where data transmitted between a sender and a recipient located in the same State are 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.

Chapter II

Legal conditions for data processing of health-related data

4. Principles concerning data processing of health-related data

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

(a) Health-related data must be processed in a transparent, lawful and fair manner;

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

(c) Data processing of health-related data should be necessary and limited to the legitimate purpose pursued and carried out in accordance with section 5;

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

(e) Health-related data must be adequate, relevant, accurate, up to date and limited to the purposes for which the data processing is to take place, and must be fit for the purposes of the data processing that is to take place;

(f) Adequate security and organizational measures must be in place for the processing of health-related data. Safeguards must guarantee respect for the rights of the data subject and the security of the health-related data. Any other guarantees may be provided for by law that safeguard respect for the rights and fundamental freedoms of data subjects and their health-related data;

(g) The rights of the data subject whose health-related data are involved in any instance of data processing must be respected. These include, but are not limited to, the rights of access to the data, information, rectification, objection, erasure and data portability. The data subject has the right to request the transmission of her or his health-related data retained by an automated processing system and/or hard copy file or records to another entity chosen by the data subject wherever technically possible for reasonable cost.

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

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

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

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

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

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

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

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

(c) For compliance with a legal obligation to which the controller is subject;

(d) To protect the vital interests of the data subject or of another natural person;

(e) For the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) For legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject that require protection of personal data, in particular where the data subject is a child;

(g) Point (f) shall not apply to processing carried out by public authorities in the performance of their tasks.

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

(a) Direct benefits to the data subject, such as health diagnosis, care, treatment, rehabilitation and convalescence of the data subject;

(b) Preventive health purposes and purposes of health diagnosis, administration of care or treatment, or management of health services by health workers and those of the social and medico-social sector, subject to the conditions provided for by law;

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

(d) To safeguard the vital interests of the data subject or of another individual where consent cannot be obtained from the data subject, the other individual, or both;

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

(f) The public interest in the accountability of the planning, funding and management of the health-care services, management of claims for social welfare and health insurance benefits and services, subject to the conditions provided for by law;

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

(h) Essential to the recognition, exercise or defence of a legal claim in relation to the health-related data intended for data processing;

(i) Essential to the identification of missing persons, or the location of a missing person (where there is no reason to believe that the individual merely wishes to avoid contact), and the circumstances raise concerns for their safety and well-being, on the basis of a law that provides for suitable and specific measures safeguarding the rights and the interests of the data subject and her or his relatives.

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

6. Health-related data of children

6.1 Health-related data and genetic data concerning children must be protected at least to the same level as other health-related data. Wherever informed consent is the legal basis for the processing of personal data of children, the child has the right to be informed and consideration must be given to the ability of the minor to fully understand the consequences of processing, and any applicable laws.

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

6.3 Children have a right to withdraw health-related data from any health information system when they reach the age of legal majority.

7. Genetic data

7.1 Data processing of genetic data may only be undertaken subject to appropriate safeguards and where it is either prescribed by law or on the basis of the consent of the data subject in accordance with paragraph 5.2, except where the law provides that a data subject cannot and/or does not need to consent to any such processing of her or his genetic data.

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

7.3 Existing predictive data resulting from genetic tests must not be processed for other purposes including insurance or law enforcement purposes, except where specifically provided for by a necessary and proportionate law.

7.4 The data subject is entitled to know or not know information relating to her or his genetic data arising from data processing of genetic data. Data subjects must be informed, prior to any data processing, of the possibility of not being informed of the results, including of any incidental findings.

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

8.1 Where health-related data are transferred by one health worker to another health worker, to provide and administer health care to an individual, that individual shall be informed before disclosure takes place, except where this proves to be impossible owing to an emergency or in accordance with paragraph 11.4.

8.2 Health-related data can, unless appropriate safeguards are provided for by law, be communicated only to an authorized recipient who is subject to rules of confidentiality.

8.3 The exchange and disclosure of data between health workers must be limited to the information necessary for the coordination or continuity of care, prevention or medico-social and social follow-up of the individual. Health workers should be able to disclose or receive health-related data necessary to care for the patient and undertake their duties.

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

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

9.1 Health-related data may be disclosed to recipients authorized and required by law to have access and possession of the health-related data to facilitate or conduct research into health issues; planning, improving and managing health-care systems;

and/or developing, evaluating or monitoring health-care activities and programmes. Such processing may be authorized only under necessary and proportionate criteria defined by law.

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

10. Storage of health-related data

10.1 Health-related data must not be stored for longer than is necessary for the purposes for which the health-related data were collected.

Chapter III

Rights of the data subject

11. Right to transparency of processing

11.1 The controller must inform the data subject of her or his right to fair and transparent processing of her or his health-related data and specifically:

(a) The identity and contact details of the controller/controllers and any processors;

(b) The source of the heath-related data being processed (where applicable);

(c) The categories of health-related data concerned;

(d) The purpose of processing, and the legal basis for the data processing of those health-related data;

(e) The length of time the health-related data will be stored or, if that is not possible, the determining criteria;

(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 in which the health-related data are obtained or to an international organization (in this case data may be transferred only to an international organization that accepts them), which shall comply with the terms of this recommendation;

(g) The possibility, if applicable, of objecting to the processing of her or his health-related data, in the conditions set out in paragraph 12.2;

(h) The conditions and the means available for exercising the rights of access, of rectification and to erasure of her or his health-related data;

(i) That data processing of her or his health-related data may subsequently occur if such data processing is for a compatible purpose or for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes, according to appropriate safeguards provided for by law and compliant with the conditions set out in paragraph 4.1 (b);

(j) The existence of automated decisions, including profiling, which is permissible only where prescribed by law and subject to appropriate safeguards, that may be made in respect of the health-related data;

(k) Any risks of the intended data processing, and the remedies available in the event of a health-related data breach;

(l) Complaint mechanisms concerning processing of her or his health-related data, including to whom such a complaint is to be made in each jurisdiction where data processing occurs;

(m) 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;

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

11.2 The information specified in paragraph 11.1 must be provided prior to the data processing of the health-related data.

11.3 The information must be intelligible, easily accessible, in plain language and suited to the circumstances to enable a full understanding by the data subject.

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

(a) The data subject already has that information;

(b) It is permitted for health-related data not to be collected directly from the data subject;

(c) The data processing of those health-related data is expressly prescribed by law;

(d) It is impossible to contact the data subject.

11.5 Where the data processing of the health-related data is for archiving purposes in the public interest, and it is impossible to contact the data subject, data processing for these purposes may be undertaken provided that the health-related data are pseudonymized or anonymized before the data processing occurs, unless otherwise provided for by law.

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

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

(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 categories of the recipients of the health-related data and the envisaged data transfers to a third country/countries, or an international organization/organizations;

(d) The period that the data-processing of the health-related data will take place, including storage;

(e) The reasoning underlying the data processing of the health-related data where the results of such data processing are applied to her or him, including for profiling, which is permissible only where prescribed by law and subject to appropriate safeguards.

12.2 Data subjects have the right to:

(a) Erasure of their health-related data processed contrary to this recommendation;

(b) Rectification of their health-related data that are inaccurate or misleading;

(c) Object to the data processing of their health-related data on grounds relating to their life and well-being. Where a controller is authorized by law to undertake data processing of health-related data notwithstanding the objection, the controller must notify the competent supervisory authority of the proposed data processing and the objection made by the data subject in a manner that will not identify the data subject (unless the data subject consents to being identified).

12.3 If rectification or erasure is rejected, the data subject must be able to review that decision, and have access to a suitable remedy if a health-related data breach has occurred.

12.4 Data subjects have the right not to be subject to decisions that significantly affect them based solely on automated processing, including profiling, of their health-related data. Derogation from this prohibition is allowed only by a law proportionate to the aim pursued, respect for the right to data protection, the right to privacy and provide for suitable and specific safeguards to protect the fundamental rights and freedoms of the data subject. Profiling for health purposes should meet generally accepted criteria of scientific validity, clinical validity and clinical utility and be subject to appropriate quality assurance programmes.

12.5 Subject to conditions prescribed by law, where the data processing of health-related data is performed by automatic means, data subjects may obtain information on the transmission from the controller, in a structured, interoperable and machine-readable format, of their health-related data, with a view to transmitting those health-related data to another controller. The data subject may also require the controller to transmit the health-related data directly to a nominated controller without delay.

12.6 The rights of the data subject may be subject to restrictions provided for by law where that law constitutes both a necessary and proportionate measure in the interests of:

(a) Protecting State security, public safety, the economic interests of the State or the suppression of criminal offences;

(b) Protecting the data subject or the rights and freedoms of others, and provides appropriate safeguards ensuring respect for the data subject's rights.

Chapter IV

Security and interoperability

13. Security

13.1 Data processing of health-related data must be conducted securely.

13.2 System availability, meaning the proper functioning of systems containing health-related data, must be facilitated with measures that enable health-related data to be accessible in a secure way and with due regard for the level of permission of authorized persons.

13.3 Guaranteeing the integrity of any data processing of health-related data requires mechanisms to enable verification of the data processing actions carried out on the health-related data; the establishment of measures to monitor access to and use of the

health-related data, to ensure that only authorized persons are able to access, use and process the health-related data. Systems containing health-related data must be auditable, to enable identification of the user(s) that undertook any specific action or data processing.

14. Interoperability

14.1 Interoperability must be in full compliance with the principles set out in this recommendation.

14.2 Reference frameworks, offering a technical framework to facilitate interoperability, must guarantee a high level of security and be audited regularly.

Chapter V

Scientific research

15.1 The processing of health-related data for the purposes of scientific research should be subject to appropriate safeguards provided for by law, comply with the provisions of this recommendation and any other rights and fundamental freedoms of the data subject, and be carried out for a legitimate purpose. No individual may be required or compelled to participate in scientific research without giving free, prior, specific and informed consent.

15.2 Consent to research participation is not valid as a consent for data processing. The conditions in which data processing of health-related data is conducted for scientific research must be assessed by a competent independent body (for example, an ethics committee or independent data custodian) that includes lay members, prior to commencement. These assessments are to be reviewed by the competent supervisory authority or another ethics committee or another independent data custodian to ensure compliance with the terms of the approval, and the fact of the approval.

15.3 In addition to consent to research participation, a separate lawful basis for data processing is required, in accordance with paragraph 15.5 of this recommendation. The lawful basis for data processing in scientific research can, but does not need to be, consent: either because the conditions for valid consent to data processing cannot be met or because the data processing is mandated by law.

15.4 The need to perform data processing of health-related data for scientific research must be evaluated in the light of the purposes of the scientific research, scientific knowledge, respect for ethical rules, purported benefits, constraints placed on the processing of the data, risks to the data subject, risks for group harm and, as concerns 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. Derogations from patients' rights for research may be used only when necessary and proportionate.

15.5 Data processing of health-related data in a scientific research project may be undertaken only if the data subject has consented to it in accordance with paragraph 5.2, except where legally provided. Any such law providing for the processing of health-related data for scientific research without the data subject's consent must be: necessary, proportionate and in the public interest; respect the right to data protection; and provide for suitable and specific safeguards to protect the rights and freedoms of the data subject. These safeguards should ensure respect for the principle of data minimization in accordance with paragraph 4.1 (e), and may include technical and organizational measures.

15.6 The data subject must, in addition to the requirements of chapter III (including but not limited to paragraph 11.1), be provided with prior, transparent and comprehensible information that is as reasonably precise as possible, on:

(a) The nature of the scientific research, the options the data subject may exercise and any relevant conditions governing the use of the health-related data, including possible re-contact and feedback of results/findings;

(b) The means and capacity to extract novel forms of health-related data and the uncertainty pertaining to what might be extractable in the future;

(c) The conditions applicable to the storage of the health-related data;

(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 under the provisions of paragraph 5.2 at any time, also that it may not be feasible to destroy health-related data already analysed and/or published before the withdrawal of consent, in accordance with paragraphs 15.11 and 15.12;

(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 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 transnational data transfer, including the legal basis for the transfer in accordance with paragraph 17.1;

(h) The publication proposed for the health-related data, and any envisaged depositing in research data repositories.

15.7 The controller should not be obliged to provide the information directly to each data subject if the conditions in paragraph 11.4 or 11.5 are satisfied. When paragraph 11.4 or 11.5 applies, the information should nevertheless be made available to data subjects in a publicly accessible way.

15.8 For scientific research where it is not possible to determine the specific purposes of the data processing at the time of the collection, data subjects should be able to express consent to data processing for certain areas of research, for certain parts of research projects or for the purpose of a biobank database, to the extent allowed by the intended purpose, with due regard for recognized ethical standards. When it becomes possible to specify the purpose further, the data subject should be informed in accordance with paragraphs 11.1, 15.6 and 15.7. Digital dynamic consent may be utilized for these purposes. This provision does not in any way reduce the requirements of consent in paragraph 5.2 as they apply to scientific research. Data subjects may also give prior consent to the future use of their health-related data for scientific research purposes after their death.

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

15.10 Where technically feasible and practicable, health-related data must be anonymized. Where it is not technically feasible and/or practicable to anonymize, pseudonymization of the health-related data, the intervention of a trusted third party

at the separation stage of the identification data, should be implemented to safeguard the rights and fundamental freedoms of the data subject. The controller cannot also function as the trusted third party. 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.

15.11 Where a data subject withdraws consent under the provisions of paragraph 5.2 or objects to the processing in accordance with paragraph 12.4, 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 contrary to law. If the destruction is contrary to law, the data subject must be informed of this and of the law requiring retention of the health-related data. Where anonymization of the data may be undertaken in a manner that does not compromise the scientific validity of the research but ensures that 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. Where the data subject continues to require destruction rather than anonymization of the health-related data, compliance is required. If the health-related data was analysed while a legal basis for the processing was in place, destruction of the data may not be practicable and may harm the integrity of the data set for the scientific research. In such cases, provided that it is vital to achieve the results of a scientific research study conducted in the public interest or where destruction would significantly affect the scientific validity of the scientific research, the health-related data processing should be strictly limited to what is necessary to achieve these purposes, but the data need not be destroyed. If it is not possible to remove data from research that has already been conducted, information about the participant should not be used for any further research.

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

(a) Where the data subject has consented to it and that consent has not been withdrawn;

(b) Where law permits such publication on the condition that it is indispensable for the presentation of research findings and only to the extent that the interest in publishing the data overrides the interests and rights and freedoms of the data subject;

(c) Where the consent of the data subject to publication of health-related data identifying that subject is withdrawn, the data controller and or processors must destroy or take down the health-related data where practicable.

Chapter VI

Mobile applications

16.1 Health-related data collected by mobile applications are covered by the same legal protection and confidentiality applicable to other health-related data under this recommendation.

Chapter VII

Transborder transfer of health-related data

17.1 Transborder transfer of health-related data may take place only where an appropriate level of data protection is met, or on the basis of one of the following provisions:

(a) The data subject has given explicit, specific and free consent to the transfer under paragraph 5.2, 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 serves important public interests, including scientific research, provided for by law and the transfer constitutes a necessary and proportionate measure;

(d) The transfer is necessary for prevailing legitimate interests pursued by the controller that are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has, on the basis of that assessment, provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in paragraph 11.1, inform the data subject of the transfer and on the prevailing legitimate interests pursued;

(e) The transfer constitutes a necessary and proportionate measure for freedom of expression.

17.2 For health-related data processed using transnational cloud computing infrastructure, platform or software, and in the absence of an obligation under international law to exercise jurisdiction, a State may exercise jurisdiction only 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;

(c) The exercise of jurisdiction is reasonable given the balance between the State's legitimate interests and other interests.

Chapter VIII

Electronic health records

18.1 All individuals have a right to privacy and the confidentiality and protection of their health-related data in electronic health record systems must be rigorously managed.

18.2 Treatment cannot be withheld by virtue of an individual not having an electronic health record.

18.3 A data subject may elect to prevent the disclosure of her or his health-related data in an electronic health record, documented by one health worker during treatment, to other health workers.

18.4 An electronic health record system must be auditable and include electronic protocols to monitor who has had access to the data in the record and access duration, logs of modification and protocols to ensure that unauthorized access does not occur and that data subjects know who has had access to their health-related data.

18.5 Evidence of a patient's consent, or withdrawal of consent, to access her or his electronic health record data is necessary. This must be electronically documented for auditing purposes.

18.6 Data processing of health-related data in electronic health record systems for the purposes of scientific research and statistical purposes is allowed where it is necessary for previously determined, specific purposes so as to protect the rights of individuals and are provided for by an existing law. Health-related data from electronic health record systems must be used for research purposes in anonymized form.

18.7 A data subject must have access to her or his health-related data in an electronic health record system. Health-related data should not be stored in an electronic health record beyond the time required for the purposes for which they were collected.

18.8 Regular auditing of access protocols in any electronic health record must take place and be reported publicly.

Chapter IX

Health-related data, genetic data and insurance

19. Health-related and genetic data and insurers

19.1 Genetic data may not be disclosed to insurers except where there is an important public interest reason provided for by law consistent with international human rights law or where the consent of the data subject has been obtained.

19.2 Health-related data and genetic data obtained for scientific research purposes cannot be used for insurance-related purposes in respect of the data subjects or their family members.

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

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

(a) The processing purpose 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 and its justification;

(b) The quality and validity of the proposed data processing of the health-related data are in accordance with generally accepted scientific and clinical standards;

(c) Data resulting from a predictive examination have a high positive predictive value;

(d) Processing is duly justified in accordance with the principle of proportionality in relation to the nature and importance of the risk in question;

(e) The quality and validity of health-related data processed for insurance purposes should meet generally accepted scientific and clinical standards.

20.2 Health-related data from family members of the insured person may not be processed for insurance purposes, unless specifically authorized by law.

20.3 The processing for insurance purposes of health-related data obtained in the public domain is not permitted to evaluate risks or calculate premiums.

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

21.1 Health-related data must not be processed for insurance purposes without the insured person's consent in accordance with paragraph 5.2.

21.2 Health-related data must be collected from the insured person.

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

22.1 Insurers may not store health-related data that are no longer necessary for the purpose for which they were 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.

23. Insurers must not require genetic tests for insurance purposes

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

23.2 Data processing of existing predictive data derived from genetic data tests may not be processed for insurance purposes unless specifically authorized by law. Where authorized, the requisite data processing is allowed only after independent assessment of conformity with the criteria in paragraph 20.1 by type of test used and with regard to a particular risk to be insured.

23.3 Existing data from genetic tests of family members of the insured person may not be processed for insurance purposes and must be destroyed by an insurer.

24. Insurers should take account of new scientific knowledge

24.1 Insurers must regularly update actuarial bases in line with relevant, new scientific knowledge and provide relevant information and justification to any insured person regarding the calculation of any premium, additional increase in premium or any total or partial exclusion from insurance.

25. States should ensure adequate mediation, consultation and monitoring

25.1 Mediation, consultation and monitoring procedures must be established to ensure the fair and objective settlement of disputes, well balanced relationship between parties and a robust evaluation of compliance with this recommendation, including by a competent supervisory authority.

Chapter X

Health-related data and employers

26.1 A controller of health-related data may include an employer. Any such employer is liable to a data subject for any health-related data breach.

26.2 An employer shall not seek health-related data from a job applicant until that applicant has been offered a job, except:

(a) To enable 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 intrinsic to the work concerned;

(c) To monitor diversity and facilitate the employment of persons with disabilities.

26.3 Employees must be informed by their employer about their rights and the purposes for the data processing of their health-related data.

26.4 Employees have the right to access their medical files to be able to verify whether they are accurate and to rectify any inaccurate or incomplete information.

26.5 Employers must make sure that the health-related data of employees is not kept for longer than necessary.

Chapter XI

Health-related data and indigenous data sovereignty

27.1 Indigenous peoples and first nations have the right to indigenous data sovereignty and indigenous governance in respect of indigenous data.

Chapter XII

Health-related data and open data

28.1 No health-related data at the unit record level may be released as open data, nor may pseudonymized data be released as open data, without the specific prior informed consent of each individual who may be affected. In the case of genetic data, an individual who may be affected includes a biological relative of the individual who is proposing to disclose her or his genetic data.

28.2 Where health-related data are released as open data and a health-related data breach arises from that release, the party that processes the health-related data and the party that releases them as open data (where they are not the same) are both liable to data subjects.

Chapter XIII

Health-related data and automated decision-making

29.1 The data subject has the right not to be subject to a health-related decision based solely on automated processing, including profiling, that significantly affects her or him. The data subject also has the right to have the original decision made by automated processing reviewed and made again by a person.

29.2 Paragraph 29.1 shall not apply if the decision:

(a) Is necessary for entering into, or performance of, a contract between the data subject and a data controller;

(b) Is authorized by a law to which the data controller is subject and which also lays down appropriate measures to safeguard the data subject’s rights and freedoms and legitimate interests;

(c) Is based on the data subject's explicit 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.

29.3 Where (a) or (c) of paragraph 29.2 applies, the controller shall implement suitable measures to safeguard the data subject's rights, freedoms and legitimate interests.

Chapter XIV

Mandatory notification of health-related data breaches

30.1 Controllers must report any significant health-related data breach to a competent supervisory authority and affected individuals not later than 72 hours from becoming aware of the health-related data breach.

Chapter XV

Right to remedy for health-related data breaches

31.1 A data subject has the right to an effective remedy, including compensation, where she or he has suffered damage as a result of a health-related data breach or the use of a medical algorithm.

Chapter XVI

Protection of reporters of health-related data breaches

32.1 Any person that honestly believes, on reasonable grounds, that a controller or other person in possession of health-related data has engaged, is engaged or proposes to engage in activity that is likely to or will result in a health-related data breach is entitled to make a protected disclosure to an independent authority and to protection from reprisal action in respect of that protected disclosure.

Chapter XVII

Liability for health-related data breaches

33.1 Member States, when assigning liability for health-related data breaches, should consider the following principles:

(a) Liability to the data subject should not be unjustifiably limited, including under tort law, to ensure that a data subject can pursue a claim for compensation against responsible entities;

(b) Patient and health worker representatives should be consulted before adopting legislation concerning liability, including any legislation governing medical algorithms;

(c) Medical algorithms should be used as a "recommendation" tool. Health workers and their organizations remain responsible to the data subject for decisions made using such tools.

Chapter XVIII

Artificial intelligence, algorithmic transparency and big data

34.1 Medical algorithms should be regulated transparently, fairly and predictably to provide:

(a) A high standard of quality, fairness, and safety (for all groups in a population);

(b) The development of technology by providing certainty to researchers, software engineers, designers, health workers and hospitals.

34.2 Requirements for all medical treatment to be monitored for efficacy of outcomes shall not be lowered to facilitate deployment or development of algorithms, big data or artificial intelligence. Forms of processing that have not yet been transparently proved in terms of their efficacy are subject to the scientific research provisions of this recommendation.

34.3 All algorithms and artificial intelligence should facilitate monitoring for adverse effects, including characteristics protected under applicable laws and United Nations conventions. This provision cannot be used to request, require or record additional demographic data.

34.4 Processes and systems must be designed and implemented to identify and address algorithmic bias. Any bias must be disclosed to data subjects and taken into account by health workers using algorithmic tools.

34.5 Any decision made using an algorithm, data or artificial intelligence should be explainable under existing requirements of the rule of law, satisfying the Rule of Law Checklist of the Venice Commission of the Council of Europe. If an algorithm is not sufficiently explainable, it can be used only in support of a decision. Any health worker who relies on such an algorithmic tool is liable for that decision.

Chapter XIX

Health-related data in non-health-care settings

35. Accessing health-related or genetic data from databases with health-care and/or research purposes for identification, judicial procedure and/or investigation

35.1 Genetic data must be collected for explicit, specific and legitimate purposes and not be processed in a manner incompatible with the purposes for which they were originally collected.

35.2 Access to health-related data or genetic data from databases that do not have a specified forensic purpose for the prevention or detection of a specific crime, or the conduct of a prosecution, must be subject to judicial oversight. Access must be provided only where necessary, proportionate and adequate safeguards exist in law to protect the rights and interests of the data subject. Access must be limited to data necessary for achieving the purpose. General access for national security or crime prevention purposes is not allowed.

35.3 Processing genetic data for criminal law enforcement purposes may be undertaken only by competent authorities for the purposes of preventing, investigating, detecting or prosecuting criminal offences where there are no alternative or less intrusive means to establish whether there is a genetic link for the

production of evidence, to prevent a real and immediate danger or for the prosecution of a specific criminal offence.

35.4 Genetic data to be used for any judicial procedure or investigation must be collected from the data subject and not be authorized by databases or biobanks that do not have a specified forensic purpose. Only in cases where it is not possible to collect the data from the data subject, access to data from databases with health-care and/or research purposes can be granted on the basis of a court order.

35.5 Genetic data can be processed for the purpose of identification of individuals in a humanitarian crisis, mass casualty event or to assist in the identification of missing persons only where appropriate safeguards are provided for by law or it is manifestly in the best interests of the individual.

36. Health-related data and immigration

36.1 Where health status is used to make decisions about lawful immigration and health-related data are collected for that purpose, the same conditions apply to the collection, use, sharing and retention of those data as apply to similar data collected from or about citizens of that State.

36.2 In the case of refugees and unauthorized arrivals a prerequisite for the collection of health-related data is dignity and integrity in the process of establishing the identity of the individual.

36.3 Authorized and non-authorized arrivals and refugees within national jurisdictions are entitled to access health-care services at no less than the minimum standards applicable to citizens in that jurisdiction.

36.4 The sharing of health-related data between international organizations responsible for the management of international migration and refugee programmes may be undertaken only where all parties to the data-sharing adhere to the provisions of this recommendation.

37. Health-related data and individuals in the care of the State

37.1 This section applies to publicly and privately funded institutions of the State. Health-related data play a vital role in the management of the lives of individuals where control over decisions about their health has been removed. These individuals are entitled to a level of health care equivalent to that provided to anyone, although institutionalization, detention or incarceration may compromise choice of services.

37.2 These principles apply in relation to individuals who are the direct responsibility of State-run or State-owned institutions and to individuals for whom this responsibility has been transferred by the State to non-State sector operators.

37.3 Access to health-related data of such individuals must comply with this recommendation and serve the interests of the individual and not be subordinated to the claimed interest of the State or institution.

38. Health-related data and marketing

38.1 Information providers and information service providers should facilitate profiling or marketing based on health-related data only if:

(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;

(c) Consent has been given and recorded, and can be withdrawn as easily as it has been given.

38.2 Third parties who collect and sell health-related data must respect data subjects' privacy and confidentiality. Linking health-related data to other identifiable data to build lists of individuals with particular illnesses or conditions requires the consent of those individuals.

38.3 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.

38.4 Health-related data collected or revealed by mobile fitness devices or applications are covered by the same legal protections and confidentiality applicable to other health-related data processing in respect of their use for profiling and marketing.

39. Health-related data and diminished capacity

39.1 The right of a person with diminished capacity to make decisions should be restricted to the least possible extent. A person with diminished capacity has a right to support for her or his decision-making.

39.2 The extent of any impairment of a person's capacity to make decisions, or the absence of the capacity to make decisions, must be established by a fair process.

39.3 A person may appoint another person or entity to make decisions for her or him. Such decisions must be made in a manner that is least restrictive of that person's rights and consistent with that person's dignity, proper care and protection.

Chapter XX

Persons with disabilities and health-related data

40.1 The rights and obligations under this recommendation apply to all individuals, including persons with disabilities. Discrimination against, or stigmatization of, persons with disabilities is unacceptable.

40.2 Individuals cannot be compelled to disclose their disability status or their health-related data relating to that disability. Where certification of the fact of disability is needed to access a benefit or service, the certification of having a disability by an authority is sufficient to establish entitlement.

40.3 Access to health-related data of persons with disabilities must meet the requirements of this recommendation and serve the interests of the individual. Access to the health-related data of a person with disabilities must be in a form accessible to that person.

Chapter XXI

Gender, gender expression and health-related data

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

41.2 Particular care in the collection and management of health-related data must be taken, including with regard to the categories used as gender markers.

Chapter XXII

Intersectionality and health-related data

42.1 Intersectionality in health care applies to practitioners and those seeking health care. The interaction of multiple factors may advantage or disadvantage individuals. Regardless of any or all of the social groups an individual is part of, every individual should be provided with the same standards of health care.

Chapter XXIII

Health-related data and notifiable diseases

43.1 Processing of health-related data necessary for reasons of public interest in the area of public health, such as reporting of notifiable diseases, is to be undertaken in accordance with chapters II and III and with suitable and specific measures in place to safeguard the rights and freedoms of individuals and to prevent discrimination against individuals.