[Place], [Date] [REFERENCE]

DRAFT RECOMMENDATION ON THE PROTECTION AND USE OF HEALTH-RELATED DATA

Table of contents

Introduction

Recommendation on the protection and use of health-related data

This document was prepared by Sean McLaughlan in his capacity as Secretary to the Task Force on Privacy and the protection of health data (MediTAS) established by the United Nations Special Rapporteur on the Right to Privacy (SRP) Professor Joseph A. Cannataci. The document was prepared under the guidance of the SRP and the Chair person of MedITAS, Professor Nikolaus Forgó, with contributions from the members of the Task Force who, in May 2019 include Teki Akuetteh Falconer, Heidi Beate Bentzen, Elizabeth Coombs, Kenneth W. Goodman, Emily Johnson, 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.

This document is Version 0.3 and is work-in-progress. [1] *This is a draft that is still work-in-progress albeit at advanced draft stage having received both written and public comments at a recent international public consultation. In particular, the introduction to the Recommendation, its referencing and acknowledgment of sources used to develop ideas contained within the document is not yet complete, but will be documented. Reliance on work compiled and completed by others has assisted greatly in compiling this document for consultative purposes. Comments and additional input is needed and requested in all areas of the document.*

The document does not reflect necessarily the view of the Special Rapporteur on the Right to Privacy nor does it represent the view of any individual member or groups of members of the Taskforce on Health Data. This draft is released for final comment following the international public consultation on 11-12 June 2019 in Strasbourg, in order to provide the opportunity for everybody to comment on the document and contribute to its completion.

[1] This document was drafted on the basis of the Draft Recommendation on the Protection of Health-related Data submitted to the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and reviewed by the Committee on its 37th Plenary meeting, Strasbourg, 20-22 November 2018.

Chapter I. General provisions

1. Purpose

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

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

2. Scope

(a)
(b)

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. See below in Section 3 definition of "data processing".

2.2 This recommendation does not limit or otherwise affect any law that grants data subjects more, wider or better rights, protection, and/or remedies than this recommendation. Where this Recommendation specifies or identifies a group of people/individuals, any provisions relating to that group/individuals are in addition to any other rights protections and/or remedies enjoyed by that people/individuals under this Recommendation or any other law.

2.3 The provisions of this recommendation do not apply to health-related data processing performed by individuals in the context of purely personal or household activities.

3. Definitions

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

- "anonymisation" means an irreversible process applied to personal data 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" should be given by 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 him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's

acceptance of the proposed processing of his or her 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 all of them. 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.

- "data processing" means any operation or set of operations which is performed on personal 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 personal data, and automatic processing of health-related data.

- "disability" is an evolving concept and that 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.[2]

- "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 from one to another. 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 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

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

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 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.[3]

- "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 and future health. Genetic data is health related data in the understanding of this Recommendation. Health-related data can be a basis for discrimination, and such discrimination may include "familial relationships" derived from health-related data. 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" intentional lawful destruction means the unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, or prevention of lawful access to, or sale of, health-related data transmitted, stored or otherwise processed; this does not include intentional lawful destruction.

- "health workers" include all people engaged in actions whose primary intent is to enhance health.[4]

- "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".[5]

- "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, genetic data, environments or resources of indigenous peoples.

- "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 Metrics Network Framework and Standards for Country Health Information Systems*, World Health Organization, January 2008.
[4] Add WHO reference.
[5] https://www.privacy-web.nl/cms/files/2017-07/handbook-data-protection-and-humanitarian-action-2-.pdf

- “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.

- “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.[6]

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

- “mobile applications” refers to means 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 objects and 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. Data must 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 which processes data on behalf of the controller.

[6] Oxford Dictionary, https://www.oxforddictionaries.com/.

- “profile” means a set of health-related data characterising a category of individuals that is intended to be applied to an individual.

- “profiling” means an automatic data processing technique that consists of applying a profile to an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.

- “pseudonymisation” 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 organisational measures so that personal data cannot be attributed or 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. [7] 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.

- transborder” means across State borders. Transborder 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.

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

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

4. Principles concerning data processing of health-related data

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

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

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

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

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

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

f. Processing of health-related data must take into consideration adequate security and organisational measures. Safeguards must be in place that guarantee respect for the rights of the data subject and the security of the health-related data. Any other guarantees may be provided for by law that safeguard respect for rights and fundamental freedoms of data subjects and their health-related data.

g. The rights of the data subject whose health-related data are involved in any instance of data processing must be respected. This includes, but is not limited to, the rights of access to the data, information, rectification, objection, and erasure. Data subjects have a right to data portability. This 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 chosen by the data subject wherever technically possible for reasonable costs.

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 the data processing, a written assessment of the potential impact of the processing of data foreseen in terms of data protection, use of data and respect for privacy of the data subjects, including of the measures aimed at mitigating all risks.

4.4 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 who are not subject to a specific level of professional secrecy such as health-care professionals 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-care professionals.

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

g. point (f) of the first subparagraph 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. there being direct benefits to the data subject such as medical diagnosis, care, treatment, rehabilitation and convalescence of the data subject;

b. preventive health purposes and purposes of medical 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 medical treatment, protection against health products and medical devices, subject to the conditions provided for by law;

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

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

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

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

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

i. reasons essential to the identification of missing persons where there is no reason to believe that the individual said to be missing merely wishes to avoid contact, and the circumstances of the person being missing raises concerns for his or her safety and well-being, on the basis of a law which provides for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject and their relatives.

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 data public.

6. Health-related data of children

6.1 In view of childrens' rights and childrens' best interest, health-related data and genetic data concerning children must be protected at least to the same level as other health-related data. Children have the same rights to privacy and data protection as adults. Wherever informed consent is the legal basis for the processing of personal data of a children, the child has the right to be informed and consideration must be given to the ability of the minor to fully understand consequences of processing, and any applicable laws. Therefore, where the child is below the age to fully understand the implications of processing, such processing shall be lawful only if and to the extent that consent is given or authorised by a legally authorized representative. However, the consent of the a legally authorized representative should not be necessary in the context of preventive or counselling services offered directly to a child, provided that the services are offered by a health-care professional acting in the best interests of the child, in circumstances where the health of the child is otherwise at risk.

6.2 Consideration should be given, once the child has reached the age of legal majority, to seek re-consent to participation in research.

7. Genetic data

7.1 Data processing of genetic data may only be undertaken subject to appropriate safeguards and where it is either prescribed by law or on the basis of the consent expressed by the data subject in accordance with the provisions of 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 to retaining and any subsequent use of the genetic data, unless otherwise provided for by any other applicable law.

7.3 Existing predictive data resulting from genetic tests must not be processed for other purposes including insurance (for example, life insurance) or law enforcement purposes, except where this is specifically provided for by law. In that case, their processing should only be authorised under appropriate and proportionate criteria defined by law, in light of the type of test used and the particular risk concerned.

7.4 The data subject is entitled to know or not know, any information relating to her or his genetic data subject to the provisions of paragraphs 11.5 and 12.7 that arise from data processing of genetic data. The data subject may have reasons for not wishing to know about certain health aspects arising from the data processing of genetic data. People must be informed, prior to any data processing, of the possibility of not being informed of the results, including of any incidental findings. The wish not to so be informed may, in exceptional

circumstances, be restricted as foreseen by law, in cases such as where a health worker has a duty to provide care or where it is in the interests of public health. An individual's wish to be kept in ignorance of a diagnosis or prognosis should be respected, except where this constitutes a serious risk to the health of third parties. The information the data subject is entitled to know under this provision does not extend to unverified research results where, in an objective assessment, providing access may be misleading.

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-care professional to another health-care professional, for the purposes of providing and administering health care of an individual, the data subject shall be informed before the disclosure takes place, except where this proves to be impossible due to an emergency or in accordance with paragraph 11.4.

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

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

8.4 In the exchange and disclosure of health-related data, physical, technical or administrative security measures must be adopted to guarantee the confidentiality, integrity, authenticity, and availability of health-related data. In the event of the failure of these measures and a health-related data breach occurs, the parties to the breach must comply with the provisions of Chapter XV of this recommendation.

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

9.1 Health-related data may be disclosed to recipients that are authorised and required by law to have access and possession of the health-related data for the purposes of facilitating or conducting research into health issues; planning, improving and managing health-care systems; and or developing, evaluating or monitoring health-care activities and programmes. Any such processing may only be authorised under appropriate and proportionate criteria defined by law, in light of the type of test used and the particular risk concerned.

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

10. Storage of health-related data

10.1 Health-related data must not be stored for longer than is necessary for the purposes for which the health-related data was processed. Where data processing of health-related data is for archiving purposes that are in the public interest, for scientific or historical research purposes or for statistical purposes, there must be appropriate measures in place to safeguard the rights and fundamental freedoms of the data subject and to prevent discrimination amongst

families, groups and populations. For these very specific purposes, health-related data may be retained beyond the period of the initial purpose of the data processing provided it is pseudonymised or anonymised as soon as reasonably practicable without materially affecting the research, archiving activity or the statistical study. In the case of archives of information held by the state, the state shall be responsible for ensuring necessary and proportionate protections of that information to prevent health-related data breaches.

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

Chapter III. The rights of the data subject

11. Right to transparency of processing

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

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 her or his health-related data, in the conditions prescribed in paragraph 12.2,
h. the conditions and the means made available to her or him for exercising via the controller her or his 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 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 paragraph 4.1.b,
j. the existence of automated decisions, 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. information required about 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. 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, namely health-related data collection.

11.3 The information must be intelligible and easily accessible, in plain language and suited to the circumstances to enable a full understanding of the data processing of the health-related data by the data subject. Where the data subject is physically or legally incapable of receiving the information, or of making a decision based on the information, it must be provided to the person legally representing her or him or the person with authority to make these decisions for the data subject. If a legally incapacitated person is capable of understanding, she or he must also be informed before the data processing of the health-related data is conducted.

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

a. the data subject already has that information, or
b. health-related data is permitted not to be collected directly from the data subject, or
c. the data processing of that health-related data is expressly prescribed by law, or
d. it is impossible to contact the data subject, namely the data subject cannot be found or is not reachable after reasonable efforts have been made.

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

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

11.5 The controller is not required to inform the data subject where data processing of health-related data is provided for by a law that is both necessary to the purpose that it is intended to achieve and proportionate in the manner it seeks to achieve this purpose with regard to the rights and freedoms of the data subject. Such laws should nevertheless 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.

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

12.1 The data subject has the right to know whether the processing of health-related data that relate 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 or countries, or an international organisation or organisations,
d. the period that the data-processing of the health-related data will take place including being stored,
e. the reasoning underlying data processing of the health-related data where the results of such data processing are applied to her or him, including in the case of profiling, which is only permissible where prescribed by law and subject to appropriate safeguards.

12.2 Data subject has the right to obtain an eraser any health-related data processed contrary to this recommendation.

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

12.4 Data subjects have the right to object to the data processing of their health-related data on grounds relating to their life and well-being. Where a controller is authorised 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 in this process). This information must be reported to the competent supervisory authority for the purposes of examining if systemic issues are arising and if unforeseen needs must be addressed.

12.5 If the request to rectify or erase the data is refused or if the data subject's objection is rejected, the data subject must be able to review that decision before a competent supervisory authority, and have access to a suitable remedy if a health-related data breach has occurred. If a health-related data breach has occurred the data controller or processor must undertake the steps provided in this recommendation relating to breach notification and the data subject may access the remedy provisions of this recommendation, or any others available to her or him in the relevant jurisdiction(s).

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

12.7 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 that health-related data to another controller (data portability). The data subject may also require the controller to transmit the health-related data directly to a nominated controller without delay.

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

12.9 The rights of the data subject may be subject to restrictions provided for by law and 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.

Any such law must provide for 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. Security measures, which should consider human rights and fundamental freedoms, must be defined and implemented to ensure that all entities conducting data processing of health-related data observe the highest standards guaranteeing the lawfulness of any data processing, and security and confidentiality of any health-related data.

13.2 Data security provisions, provided for by law or other regulations, and which may be contained in reference frameworks, may require technical and organisational measures, that must be regularly reviewed, to protect health-related data from any health-related data breach. The law must make provision for organising and regulating procedures concerning the collection, storage and restitution of health-related data.

13.3 System availability, meaning the proper functioning of systems containing health-related data, must be facilitated with measures that enable the health-related data to be made accessible in a secure way and with due regard for the level of permission of authorised persons. Such system availability is to be considered in the context or emergency situations to ensure system availability and integrity of health-related data, including access by the data subject.

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

13.5 External data hosting of health-related data must ensure the security of the health-related data and comply with all principles of personal data 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. In cases where they do not, the health-related data should be dealt with in line with the provisions of this recommendation.

13.6 Persons not directly involved in the individual's health care, including employees undergoing training, but by virtue of their assigned tasks enable the operation of information systems, may have access, insofar as this is necessary for the fulfilment of their duties and on an ad hoc basis, to health-related data in an information system. Such professionals must have full regard for the confidentiality of the information, any applicable professional secrecy and 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.

14. Interoperability

14.1 Interoperability must be carried out in full compliance with the principles provided for by this recommendation, in particular the principles of lawfulness, necessity and proportionality and that data protection safeguards be put in place when using interoperable systems.

14.2 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 V. Scientific research

15. 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 with 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 their prior consent.

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

In addition to consent to research participation, a separate lawful basis for data processing is required according to paragraph 15.3 of this Recommendation. In line with paragraph 15.3 of this Recommendation, the lawful basis for data processing in scientific research can, but does not need to, be consent. In some cases, consent to data processing for scientific research purposes is not an option, either because the conditions for valid consent to data processing cannot be met, or because the data processing is mandated by law. Where consent is used as the legal basis for the data processing, dynamic digital consent solutions may be particularly

well suited to maintain the validity of the consent for data processing in dynamic scientific research.

15.2 The need to perform data processing of health-related data for scientific research must be evaluated in light of the purposes of the scientific research, the state-of-the-art of scientific knowledge, respect for ethical rules presiding the research domain, the purported benefits, the constraints placed on the processing of the data, the risks to the data subject, the risks for group harm, and, as concerns the processing of genetic data, the risk to the biological family that share some of that genetic data with the data subject and the risks of identifying non-paternity or other unexpected familial relationships. Any derogations from patients' rights for research may only be used when necessary and proportionate.

15.3 Data processing of health-related data in a scientific research project may only be undertaken if the data subject has consented to it in accordance with the provisions of paragraph 5.2 of this Recommendation, except where provided for by law. 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. Such a law must be proportionate to the aim pursued, respect the right to data protection and provide for suitable and specific safeguards to protect the rights and freedoms of the data subject. These safeguards should ensure respect for the principle of data minimisation according to paragraph 4.1(e) of this Recommendation. This may include technical and organisational measures to ensure purpose limitation, deletion, destruction, pseudonymisation and anonymisation of data at the earliest opportunity consistent with the law and other access approvals.

15.4 The data subject must, in addition to what is required by Chapter III of this Recommendation (including but not limited to paragraph 11.1), be provided 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;
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 paragraph 5.2 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 paragraphs 15.9 and 15.10 of this Recommendation; and
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; and
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; and
g. planned transnational data transfer, including the legal basis for the transfer according to paragraph 17.1 of this Recommendation; and

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

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

15.6 For scientific research, including biobanks' databases, where it is not possible to determine the specific purposes for the data processing at the time of the collection of data, data subjects should be able to express consent to data processing for certain areas of research or certain parts of research projects or the biobank's database's purpose, to the extent allowed by the intended purpose, with due regard for recognised ethical standards. When it becomes possible to specify the purpose further, the data subject should be informed in accordance with paragraphs 11.1, 15.4 and 15.5 of this Recommendation. Digital dynamic consent may be utilized for these purposes. This provision does not in any way reduce the requirements of consent in paragraph 5.2 of this Recommendation 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.[8]

15.7 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.

15.8 Where it in relation to the scientific research purposes is technically feasible and practicable, health-related data must be anonymised. Where it in relation to the scientific research purposes is not technically feasible and/or practicable to anonymise, pseudonymisation of the health-related data, with the intervention of a trusted third-party at the separation stage of the identification data, should be implemented to safeguard the rights and fundamental freedoms of the data subject. The controller cannot also function as the trusted third-party. 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.

15.9 Where a data subject withdraws consent according to paragraph 5.2 of this Recommendation or objects to the processing according to paragraph 12.4 of this Recommendation, health-related data about the data subject processed in the course of that scientific research must be destroyed in compliance with the wishes of the data subject unless to do so would be contrary to law. If the destruction is contrary to law, the data subject must be informed of this and of the law requiring retention of the health-related data. Where anonymisation of the data may be undertaken in a manner that does not compromise the scientific validity of the research but ensures the data subject cannot be identified even with the use of other data sets, this may be undertaken as an alternative to destruction and the data subject should be informed accordingly. Where the data subject continues to require destruction rather than anonymisation of the health-related data, this must be complied with. 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

[8] Consider provisions of the *Human Tissue Act 2004* (UK).

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 it necessary to achieve these purposes, but need not be destroyed. If it is not be possible remove data from research that has already taken place, information about the participant should nevertheless not be used for any further research.

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

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

b. where law permits such publication on the condition that this is indispensable for the presentation of 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 data controller and or 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 research.

Chapter VI. Mobile applications

16. Mobile applications

16.1 Where the data collected by mobile applications, whether implanted on the data subject or not, may reveal information on the physical or mental state of an data subject in connection with the data subject's health or concern any information regarding health care, they constitute health-related data. In this connection they enjoy the same legal protection and confidentiality applicable to other health-related data processing as provided by this Recommendation and, where applicable, supplemented by law.

16.2 Individuals using such mobile applications, as soon as they involve the data processing of their health-related data, enjoy the same rights as those provided for in Chapter III of this Recommendation. The individual must notably have obtained beforehand all necessary information on the nature and functioning of the system, as well as risks, such as health risks and security risks, in order to be able to control its use. To this effect clear and transparent information on the intended processing should be drafted by the controller with the participation of the software designer whose respective roles have to be determined in advance.

16.3 Any use of mobile applications must be accompanied by security measures that provide for the authentication of the person concerned, the encryption of the transmitted health-related data, and user or patient information standards on how the health-related data that is collected will be used. Mobile applications should be designed to be usable by anyone and to protect health-related data also to outside observers so that the information that the mobile application is installed or its interaction with a backend server is not an indication of the user's health status.

16.4 Any external hosting of health-related data produced by mobile applications must comply with security rules providing for the confidentiality, integrity, access and restitution of the data upon request of the data subject.

Chapter VII. Transborder transfer of health-related data

17. Protecting health-related data transfers

17.1 Transborder transfer of health-related data may only take place where an appropriate level of data protection is met, or on the basis of the following provisions aimed at allowing a transfer that does not ensure such an appropriate level of protection:

a. the data subject has given explicit, specific and free consent to the transfer according to paragraph 5.2, after being informed of the applicable law and risks arising in the absence of an appropriate safeguards level of data protection; or

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

c. the transfer serves important public interests, including scientific research, provided for by law and the transfer constitutes a necessary and proportionate measure; or

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

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

17.12 For health-related data processed in transnational 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.[9]

Chapter VIII. Electronic Health Records

18. Protecting health-related data in 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 (EHR) systems, both institutional and cross-institutional, must be rigorously managed according to data protection, ethical, professional,

[9] Heidi Beate Bentzen & Dan Svantesson, Jurisdictional Challenges Related to DNA Data Processing in Transnational Clouds, in Dan Svantesson & Dariusz Kloza (eds.), Trans-Atlantic Data Privacy Relations as a Challenge for Democracy, Intersentia Ltd (2017); 241-260

legal and all other applicable requirements by all health-care professionals and any person dealing with EHR systems. No health-related data in an EHR is to be destroyed where to do so would be in contravention of another law that is necessary and proportionate. These provisions are consistent with the right of the data subject to withdraw consent at any time of the data processing (or "opt-out"), as set out in this recommendation.

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

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

18.4 A data subject may elect to prevent disclosure of her or his health-related data in an EHR, documented by one health-care professional during treatment, to other health-care professionals, if she or he chooses to do so.

18.5 An EHR system must be auditable and include electronic protocol of who had access to data in an EHR, duration of that access, logs of modification and protocols to ensure unauthorised access does not occur and that data subjects know who has had access to their health-related data.

18.6 Data processing of health-related data in an EHR may only be undertaken by health-care professionals and authorised personnel of health-care institutions who are involved in the data subject's treatment. There must be a relationship of actual and current treatment between the data subject and the health-care professional wanting access to health-related data in her or his EHR. Any other health-care professional seeking access to health-related data of the data subject in an EHR must have the prior consent of the data subject. There must also be common standards for data accuracy and quality for all health-related data stored in an EHR.

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

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

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

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

18.11 Data processing of health-related data in EHR systems for the purposes of medical scientific research and statistical purposes is allowed where they are necessary for previously determined, specific purposes under special conditions and guarantee proportionality so as to protect the fundamental rights and the privacy of individuals and are provided for by an existing law. Health-related data from EHR systems have to be used for research purposes in anonymised form wherever possible.

18.12 A data subject must have access to health-related data that relates to them that is in an EHR system. Access must be given without undue delay or expense. EHR systems may have many different data controllers, and where there is more than one controller, a single entity must be made responsible to data subjects for the proper handling of access and other requests about the EHR. Health-related data should not be stored in an EHR beyond the time required for the purposes for which it was collected.

18.13 Regular internal and external auditing of access protocols in any EHR must take place and be reported publicly. Entitles that use EHR systems must have data protection officers to assist data subjects and health care professionals to meet their obligations in respect of the EHR.

18.14 No health insurance company may be granted access to the EHR of a data subject. Access to information that is required by law to be given to private insurance companies may be provided by the use standard protocols within EHR systems and transmitted electronically to the insurance company with the prior consent of the data subject if provided for by law.

Chapter IX. Health-Related Data, Genetic Data and Insurance

19. Health-related/Genetic data and insurers

19.1 Genetic data linked to an identifiable person may not be disclosed or made accessible to third parties, in particular, employers, insurance companies, educational institutions and the family of the individual, except where there is an important public interest reason in cases restrictively provided for by domestic law consistent with the international law of human rights or where the consent of the data subject has been obtained as stipulated by domestic law, the international law of human rights and paragraph 5.2 of this Recommendation. The privacy of a data subject participating in a study using human genetic data, human proteomic data or biological samples must be protected and the data must be treated as confidential.

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 from which it was obtained, or the biological family members of those data subjects.

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. “Relevance” refers to the value of the information recognised as appropriate for assessing the state of health of an insured person and evaluating the risks relating to his or her future health. The results of an examination with predictive value do not per se fulfil the criterion of relevance, as the reliability of the results of examinations with a predictive value is extremely variable from one examination to another;
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; and
e. the quality and validity of health-related data processed for insurance purposes should meet generally accepted scientific and clinical standards. Such data may include already existing health-related data resulting from examinations previously carried out as well as data resulting from examinations requested by insurers. In both cases, the examinations concerned must comply with generally accepted scientific and clinical criteria and be used in clinical practice. It is essential in this context that the interpretation of the data is of high quality.

20.2 Health-related data from family members of the insured person should not be processed for insurance purposes, unless specifically authorised by law. If so, the criteria laid down in paragraph 19.1 and the restriction laid down in paragraph 22.3 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.

20.3 The processing for insurance purposes of health-related data obtained in the public domain, such as on social media or internet fora, is not permitted to evaluate risks or calculate premiums.

20.4 The processing for insurance purposes of health-related personal data obtained in a research context involving the insured person is not permitted.

20.5 Questions posed by the insurer 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 documents relating to the collection of health-related data.

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 free, express and informed consent in accordance with paragraph 5.2.

21.2 Health-related data must be collected from the insured person by the insurer. The transmission of health-related data by a third party may only be made with the prior free, express, informed and explicit consent of 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 which is no longer necessary for the accomplishment 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.

22.2 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.

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

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 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 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 if comes within the purview of the insurer.

24. Insurers should take account of new scientific knowledge

24.1 Insurers must regularly update their actuarial bases in line with relevant, new scientific knowledge.

24.2 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.

25. States should ensure adequate mediation, consultation and monitoring

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

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

25.3 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 X. Health-related data and employers

26. Health-related data and employers

26.1 A controller of health-related data may include an employer[10], and the obligations of controllers in this recommendation apply to employers that are controllers. Any health-related data breach for which an employer is liable as a controller will allow the employee or data subject affected by the breach access to remedies available in this Recommendation, and possibly elsewhere. An employer may process relevant health-related data relating to

[10] Need to consider if this will apply to all employers, or if, say, SMEs may need to be excluded from some of the following provisions.

employees (such as medical certificates and other medical data) provided that they comply with the requirements of this Recommendation.

26.2 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:

(i) to enable the employer to make reasonable adjustments to the place of work to facilitate the employment of the individual;
(ii) to establish whether the applicant can carry out a function that is intrinsic to the work concerned;
(iii) to monitor diversity and facilitate the employment of disabled persons.

26.3 Employees must be informed by their employer about their rights and what the purposes are for the data processing of their health-related data. Such information must be specifically communicated to employees when a new procedure is introduced and made permanently available. This ensures that staff members have access to the information at all times.

26.4 Employees have the right to access their medical files and other health-related information 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.

26.5 Employers must make sure that information relating to health of employees is not kept on their files for longer than necessary. Clear retention periods must be established. These can vary in accordance with the reason for processing the health data.

26.6 Due to its sensitivity, health-related data may only be processed by health-care professionals bound by the obligation of medical secrecy, or other professional bound by similar obligations of secrecy, such as lawyers and legal professional privilege. All human resources staff dealing with administrative or financial procedures in this respect should sign a specific confidentiality declaration and they should be reminded of their confidentiality obligations regularly. Furthermore, organisations should carry out a risk assessment and develop, where necessary, specific security measures on access control and management of all the information processed in the context of health data.

Chapter XI. Health-related data and Indigenous Data Sovereignty

27. Health-related data and Indigenous Data Sovereignty

19
20

27.1 Indigenous peoples have the right to:

a. Exercise control of health-related data that relates to indigenous peoples. This includes the creation, collection, access, analysis, interpretation, management, security, dissemination, use, reuse infrastructure and all other data processing of health-related data relating to indigenous peoples.
b. Access and be consulted on health-related data of indigenous peoples that is contextual and disaggregated (available and accessible at individual, community and first nations levels).

c. Health-related data of indigenous peoples that is relevant and empowers sustainable self-determination and effective self-governance for indigenous peoples and first nations.
d. Health-related data structures that are accountable to indigenous peoples and first nations.
e. Health-related data that is protective and respects the individual and collective interests of indigenous peoples and first nations.
f. Decide which sets of health-related data require active governance involving indigenous peoples.
g. Exercise indigenous data governance and indigenous data sovereignty in respect of health-related data and the data processing of health-related data that relates to indigenous peoples.
h. Decisions about the physical and virtual storage of health-related data relating to indigenous peoples shall enhance control for current and future generations of those indigenous peoples. Whenever possible, health-related data relating to indigenous peoples shall be stored in the country or countries where the indigenous people to whom the data relates consider their traditional land to be.
i. The ability to disaggregate health-related data of indigenous peoples increases its relevance for the communities and other traditional groupings of indigenous peoples. Health-related data of indigenous peoples shall be collected and coded using categories that prioritise the needs and aspirations of indigenous peoples as determined by them.
j. The collection, use and interpretation of data shall uphold the dignity of indigenous communities, groups and individuals. Data processing of health-related data that stigmatises or blames indigenous peoples can result in collective and individual harm and should be actively avoided.

27.2 Indigenous data governance enables indigenous peoples, representatives of indigenous peoples and governing bodies of indigenous peoples to ensure that health-related data is accurately dealt with. Indigenous data governance provides indigenous peoples and first nations with the necessary tools to identify what works, what does not and why in respect of indigenous peoples. Effective indigenous data governance empowers indigenous peoples to make, or be more involved in making, decisions to support communities and first nations in the ways that meet development needs and aspirations of these communities. States must provide indigenous data governance to indigenous peoples within their territorial boundaries.

Chapter XII. Health-related data and Open Data

28. Health-related data and Open Data

28.1 The consequences of disclosure of health-related data present greater risks to the individual in terms of discrimination and other consequences, no health-related data at the unit record or patient/person level may be released as Open Data, nor may pseudonymised data be released as Open Data, without the specific prior informed consent of each individual that may be affected. In the case of genetic data, an individual that may be affected includes a biological family member of the individual that proposes to disclose their genetic data.

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

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

Chapter XIII. Health-related data and automated decision making

29. Health-related data and Automated Decision Making

29.1 The data subject shall have the right 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 her or him. The data subject shall also have the right to have the original decision made by automated processing to be reviewed and made again by a human. The data subject has a right to have any decision made in reliance or in part on their health-related data explained to them by a competent person how any automated decision-making technology works, the factors that lead to the decision that has or will be made, and for necessary information to be provided that will justify any decision that has been or will be made.

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 authorised 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; or
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 In the cases referred to in points (a) and (c) of paragraph 29.2, 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 her or his point of view and to contest any decision.

Chapter XIV. Mandatory Notification of Health-Related Data Breaches

30. Mandatory Data Breach Notification of Health-related data breaches

24
25
Controllers must report any 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 data breach[11].

a. describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

[11] The issue of a threshold requirement is being considered - eg the breach must be of a specific level of seriousness before reporting is required to avoid reports of technical health related data breaches.

b. communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
c. describe the likely consequences of the personal data breach;
d. describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Chapter XV. Right to Remedy for Health-Related Data Breaches

31. Right to Remedy for Health-related data breaches

22
23
31.1 Without prejudice to any available administrative or non-judicial remedy, a data subject has the right to seek an effective judicial remedy where he or she considers that her or his rights under this recommendation have been infringed as a result of the data processing of her or his health-related data in non-compliance with this recommendation, or they have suffered a health-related data breach.

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

31.3 Any person who has suffered material or non-material damage as a result of an infringement of this recommendation or health-related data breach shall have the right to seek compensation from the controller or processor for the damage suffered.

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

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

Chapter XVI. Protection of Reporters of Health-related Data Breaches

32. Protection of reporters of Health-related Data Breaches

27
28
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-data breach, is entitled to make a protected disclosure to the competent supervisory authority in connection with that information.

32.2 Any person that makes a protected disclosure concerning health-related data under paragraph 31.1 is entitled to protection whereby it is an offence to take reprisal action against

the individual for having made the protected disclosure concerning health-related data breaches.

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

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

Chapter XVII. Liability

33. Liability for Health-related data breaches

33
34
33.1 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.

33.2 Medical algorithms should be regulated in a transparent, fair and predictable manner in order to provide;

a. data subjects harmed by such technology with an avenue of compensation;
b. a high standard of quality and safety of algorithms; and
c. the development of such important technology by providing certainty to researchers, software engineers and designers, and to health workers and hospitals.

33.3 Member States, when drafting legislation and determining how to assign liability to entities and individuals involved in the creation and use of algorithms, should keep the following important principles in mind:

a. Patient and health worker representatives should be consulted before adopting legislation governing algorithms.
b. Algorithms should be used as a “recommendation” tool. The health workers should make the final care or diagnostic decision. That is, a healthcare professional should always review the algorithm’s output.
c. The health worker or end user of the algorithm should be required to educate herself or himself about the general structure or methodology the algorithm employs to come to its conclusion, and the key independent variables the algorithm the model takes into account (e.g., age, sex, blood pressure, etc.).
d. If health workers employing algorithms should be required to inform patients that the health care professional is employing such methods and make the patient aware of the risks associated with the use of such technology. If the healthcare professional(s) should be required to give a patient information about the use of algorithms in his or her care, how much information the health worker should be required to provide the patient about the algorithm and how it is employed.

e. If algorithms should be required to pass certification requirements or should undergo standard validation of performance tests (e.g., testing the rate at which the algorithm correctly predicts pre-specified outcomes, peer review).
f. If warnings should be required when algorithms are used in medical care.
a. Potentially novel methods of compensating patients for harm caused by black box algorithms: One potential approach would be to tax to charge a fee every time an algorithm is used during the course of medical treatment and then to create a State-administered fund. This approach makes it possible to compensate patients without assessing the fault of the treating healthcare professional versus the algorithm and avoids the costly exercise of litigating or otherwise determining whether an algorithm was faulty.

b. Whether to employ a publicly administered licensing scheme for black box algorithms. That is, require the algorithm to demonstrate certain safety features before it is used commercially and permit revocation of a license if the algorithm exceeds a certain number of "errors" or false positives/negatives.

Chapter XVIII. AI, Algorithmic transparency and Big Data

34. Algorithmic transparency and fairness

34.1 Medical algorithms are often used to "perform" tasks that normally require human intelligence. Medical algorithms are used to, for example, predict patient risks (e.g., for hospital readmission), make accurate diagnoses (e.g., does an x-ray show cancer or not?), select what medicine to administer, or to assign limited health resources. Black box algorithms are a subcategory of such technology whose methods at arriving at a conclusion are opaque to humans. This is either because a black box algorithm's decision making process is "too complex" for humans "to explicitly understand" or because "the relationships used in a black-box algorithm are literally unknowable because of the machine-learning techniques employed – that is, no one, not even those who programmed the machine –learning process, knows exactly what factors go into the ultimate decisions

34.2 Requirements for all medical treatment to be monitored for efficacy of outcomes are longstanding. Standards shall not be lowered to facilitate deployment of data processing technology, whether that be algorithms, big data or AI, as they were not previously for instrument sterilisation, or electricity. Forms of processing that have not yet transparently proved their efficacy shall be subject to the scientific research provisions of this recommendation.

34.3 All algorithms, and all versions of AI and machine learning algorithms, should facilitate monitoring for adverse effects by the health-care professionals and their organisations, with special attention paid, where such data is available, to characteristics protected under applicable UN Conventions and local laws. This provision should not be used to request, require, or record additional demographic data on any patient.

34.4 All algorithms, and all versions of AI and machine learning algorithms must be fair. Processes and systems must be designed and implemented to identify any potential implicit algorithmic bias. Where possible, steps must be taken to address any bias. Any bias must be

disclosed to data subjects who may be unfairly assessed by the algorithm. Health workers must take biases into consideration when using algorithmic tools.

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

34.5 Data sets on populations, or subsets of populations, may affect different subgroups with disproportionate consequences, whether through their inclusion or exclusion from health systems. Data derived from such systems may not be representative of a wider population. While a health worker or their organisation may treat only a subset of a local population, it remains their responsibility to ensure that any algorithms, data, or AI used will not cause undue harm to the population as a whole. Compatibility with UN Conventions and Declarations must be maintained for all.

34.6 Any decision made an algorithm, data, or AI, should be explainable to the standards of decision making under existing commitments to the Rule of Law, and in practice, satisfying the Venice Commission of the Council of Europe's Rule of Law Checklist. If an algorithm is not sufficiently explainable, it can only be used in support of a decision. Any health worker that relies on a non-transparent algorithmic tool in support of a decision affecting a patient carries the professional responsibility for the decision.

25
26

Chapter XIX. Health-related Data in non-healthcare settings

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

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

35.2 Access to health-related 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 and specific approval by a court. Such access must only be provided where it is necessary and proportionate and where adequate safeguards exist in law to protect the rights and interests of the data subject. The procedures for obtaining access must be made publically accessible to all participants in the database. The access must be limited to data strictly necessary for achieving the purpose. General access for national security or crime prevention purposes is not allowed. Access to health-related or genetic data cannot be provided for identifying individuals with genetic propensities for criminal activity for preventive purposes.

35.3 In the context of processing genetic data for criminal law enforcement purposes, such uses must only be possible for competent authorities (for the purposes of preventing, investigating, detecting or prosecuting criminal offences or executing criminal offences). Data processing of genetic data for the purpose of a judicial procedure or investigation may be

undertaken only when there are no alternative or less intrusive means to establish whether there is a genetic link for the production of evidence, to prevent a real and immediate danger or for the prosecution of a specific criminal offence.

35.4 Genetic data to be used for the purpose of any judicial procedure or investigation must be collected from the data subject and not be authorised 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. The database custodian maybe given the opportunity to provide reasons for objection to access to the database, on behalf of the participants.

35.5 Genetic data which are processed for the purposes of judicial proceedings, such as to determine biological kinship, should be used only to establish whether or not a genetic link between the individuals exists. Such genetic data may not be used to determine other characteristics of the data subject, nor may such genetic data, or health-related data, or personal data derived from that genetic data be retained beyond the necessary time period to complete the original purpose of the data processing of the genetic data.

35.6 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 (in accordance with para 5.1i), only where appropriate safeguards are provided for by law or it is manifestly in the best interests of the individual. Persons, and groups, in need of humanitarian assistance retain their right to privacy, which may be particularly important in e.g. refugee camps and conflict zones, where identification of a person's family members or ancestry may put them especially at risk, including in future political scenarios. Data from the family members of a missing or deceased person may only be processed if the data subject has given her or his free, specific, informed and explicit consent to that data processing. Genetic data should not be retained beyond the necessary time period to complete the original purpose of the data processing of the genetic data. Only in cases where it is not possible to collect the data from the data subject or their family, genetic data held in databases with health care and/or research purposes may be accessed for these identification purposes on the basis of a court order. Such access must only be provided where it is necessary and proportionate and where adequate safeguards exist in law to protect the rights and interests of the data subject. The procedures for obtaining access must be made publicly accessible to all participants in the database. The access must be limited to data strictly necessary for achieving the purpose.

36. Health-related data and immigration

36.1 Health-related data within the context of national and international immigration policies and arrangements involves the complex interaction of three policy streams: human rights and international conventions; domestic immigration, population and border control polices and issues of access to the provision of public health services.

36.2 There are different legal obligations cast upon nation-states who are signatories to the Convention Relating to the Status of Refugees 1951 and or/ its 1967 Protocol, and those who are not.

36.3 Similarly, states may adopt different policies in relation to individuals who are classified as authorised arrivals and those who are unauthorised (prohibited non-citizens).

36.4 There are however fundamental requirements that all individuals be treated according to the principles enshrined in universal declarations of human rights and international covenants regarding human rights and freedoms and the right to health care.

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

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

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

36.8 Authorised arrivals, non-authorised arrivals and refugees within national jurisdictions are entitled to access health care services at no less than the minimum standards accessible to citizens within that jurisdiction. Health-related data should be collected, used, shared and retained to the extent necessary to facilitate access to such care. No individual, regardless of their immigration or refugee status may be denied or deprived of access to minimum standards of health care.

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

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

37.1 Individuals may be in institutional care of the state because of their age, their health status or because of their criminal behavior. They may be wards of the state; involuntarily placed in care facilities or sentenced to detention or prison. The provisions in this section applies to both publically and privately funded institutions. Health 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.

37.2 It is a fundamental principle that people in such circumstances are entitled to a level of health care equivalent to that provided to anyone else in their wider community. Institutionalisation, detention or incarceration in no way diminishes that fundamental right, although it is recognized that such status may compromise their level of choice of such services.

37.3 These principles apply equally in relation to individuals who are the direct responsibility of state-run or state-owned institutions and to individuals where this responsibility has been transferred by the state to the non-state sector operators.

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

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

37.6 Particular care in the collection and management of their health data, must be taken where such individuals are not able, either as a result of their age, their own medical or psychiatric condition, or because they are under the control of custodial authorities, to exercise any meaningful form of informed consent. This principle must be particularly considered when dealing with requests for research to be carried out on such populations, or subsets thereof.[12]

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

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

38. Health-related data and Marketing

38.1 The use of health-related data for marketing is generally incompatible with privacy obligations.

38.2 Any use of health-related data for marketing purposes should be based solely upon free, specific, informed and explicit consent, except where the law provides that a prohibition on health-related data processing for marketing purposes cannot be lifted by the data subject's consent.

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

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

38.5 Respect for the privacy and confidentiality of health-related data is incompatible with individual profiling or targeting for marketing or financial gain.

38.6 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:

[12] Reference here to Helsinki Declaration

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. free, specific, informed and explicit consent has been given and recorded, and can be withdrawn as easily as it has been given.

38.7 Information intermediaries, data brokers, or other third parties who collect and sell 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 free, specific, informed and explicit consent of the individuals concerned.

38.8 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.

38.9 Data collected by mobile fitness devices or apps may reveal information on the physical or mental state of an individual and therefore constitutes health-related data. It should therefore enjoy the same legal protections and confidentiality applicable to other health-related data processing in respect of its use for profiling and marketing. All necessary information on the nature and functioning of the device, app or system must be provided in order for the data subject to be able to control both its use and the use of the data which it generates and/or transmits.

38.10 Where suspected or inferred conditions might tend to make individuals more vulnerable (e.g. through cognitive impairment) it is entirely incompatible with human rights obligations to permit profiling or targeted marketing of such vulnerable persons.

39. Health-related data and diminished capacity

39.1 A person's right to make decisions is fundamental to that person's dignity. The right to make decisions that each person has also applies to decisions regarding a person's health-related data. The right extends to the ability to make decisions about the health-related data of that person with which others might not agree.

39.2 The right of a person with diminished capacity to make decisions about their health-related data should only be restricted, or otherwise interfered with, to the least possible extent. A person with diminished capacity to make decisions has a right to adequate and appropriate support for their decision-making about their health-related data.

39.3 The capacity of any person to make decisions about their health-related data may differ according to the nature and extent of any impairment affecting their capacity to make decisions. In addition, the nature of a decision to be made about their health-related data may be relevant to capacity to make decisions. This may be the case because of factors such as the complexity of the decision to be made, or the expected length of time for which the consequences of the decision may affect the individual. These factors may include the possibility of the effect of any decision being able to be undone should the person regain capacity to make such decisions and wish to revisit the decision made. The support available from members of the person's existing support network may also affect the types of decisions people with diminished capacity are able to make, or the method by which decisions for the individual may be made (meaning

they may involve an extended support group making or being involved in making, decisions for that person).

39.4 Any person that is not a minor, is presumed to have the capacity to make decisions about their health-related data. It must be established by evidence that a person does not have the capacity to make decisions about their health-related data, or the extent to which their decision-making capacity about their health-related data is impaired. Also, the nature or type of decisions about health-related data that a person may not be able to make must be established by evidence. If a person has made a decision about their health-related data in the past when they had the requisite capacity to make that decision, that decision may not be overturned by virtue of their having ceased to have capacity subsequent to the making of that decision. A person may appoint another person or entity to make decisions for them concerning their health-related data.

39.5 The importance of encouraging and supporting a person with diminished capacity to make decisions to achieve their maximum physical, social, emotional and intellectual potential, and to become as self-reliant as practicable, must be taken into account when determining what decisions that individual is able to participate in making about their health-related data. The development, self-reliance and rights of the person must also be taken into account, when determining the extent of the participation of an individual in the decision-making process concerning their health-related data.

39.6 A person's right to participate, to the greatest extent practicable, in decisions affecting their health-related data, must be recognised and taken into account. The importance of preserving, to the greatest extent practicable, a person's right to make their own decisions about their health-related data must be taken into account. The person must be given any necessary support, and access to information, to enable the person to make, or participate in making, decisions affecting their health-related data.

39.7 A person or other entity making a decision about health-related data for a person with diminished capacity must do so in a manner that is least restrictive of the person's rights. Where it is reasonably practicable to work out what a person's views and wishes would be for their health-related data in a given situation because of the previous actions of that person, a person or other entity making a decision that will affect that person must take into account what the person or other entity considers would be the views and wishes of the person with diminished capacity.

39.8 A person or other entity making a decision for a person with diminished capacity that relates to their health-related data must do so in a way consistent with that person's proper care and protection. This includes the possibility that the participation of the person in any decision or decision-making process that may adversely affect their health or well-being. The views and wishes of a person may be expressed orally, in writing or in any other way, including, for example, by conduct.

39.9 The importance of maintaining a person's cultural and linguistic environment, and set of values (including any religious beliefs), in so far as they relate to health-related data, must be taken into account except where that person has expressly, through writing, words or other conduct, indicated that they do not wish for it to be. This includes traditional forms of communal decision making where the individual or their decision maker has indicated that they wish for these traditional forms of communal decision making to be followed in relation to decisions made about their health-related data.

39.10 Where power over decision making that relates to health-related data is exercised by another person for a person with diminished capacity, that power must be exercised in a way that recognises the dignity of the person and is appropriate to that person's characteristics and needs as they relate to their health-related data. To the greatest extent practicable, the views of the person for whom, or in respect of whom a decision is to be made by another person or entity, must be obtained by that person or entity making the decision before any decision is made except where to do so might cause harm to, or exacerbate the condition of, the person with diminished capacity.

39.11 Where power is exercised by another person for a person with diminished capacity, that power may not be exercised where that person has a conflict of interest (direct or indirect) in the decision to be made. In such cases the conflict must be managed to preserve the rights of the individual for whom the decision is to be made. The views of the person for whom, or in respect of whom, a decision is to be made by another person or entity, must be obtained where practicable to do so, on any conflict of interest identified before any decision is made, except where to do so might cause harm to, or exacerbate the condition of, the person with diminished capacity. Where harm may be caused, or the condition of the person may be exacerbated, by involving the individual with diminished capacity in the decision-making process and their consent cannot be obtained to participate in trials or studies, that individual cannot participate in the proposed trial or study for which a decision is required regardless of the powers granted to the individual or individuals empowered to make decisions for the individual with diminished capacity.

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

39.13 A person's right to confidentiality of information about that person including their health-related data must be recognised and taken into account. This includes health-related data about the diminished capacity of the person.

39.14 A person with diminished capacity has the same rights and obligations granted under this document as any other person. The provision of decision-making powers to another person or entity in the case of diminished capacity does not obviate any other provision in this document nor does it render any decisions made by the person deemed to have diminished capacity of no effect unless such a finding indicates that the decision was made while the person had diminished capacity to make it, and that harm is being caused to that person as a result of that decision.

Chapter XX. People Living with Disabilities and Health-related data

40. People living with disabilities and Health-related data

40.1 The rights and obligations granted under this document apply to all individuals including persons with disabilities. The provisions outlined in this guidance are to be maintained without discrimination on the basis of whether or not a person is living with a disability.

40.2 States parties have a responsibility to observe the provisions of the Convention of the Rights of Persons with Disabilities.

40.3 People, regardless of issues of disability are entitled to equal treatment/access/standards (with all others) in line with the principles established elsewhere throughout this document.

40.4 The definition of disability may be culturally constructed but what is essential is respect for the dignity of and respect for each individual as a person.

40.5 Any form of discrimination against or stigmatisation of (and especially any form of physical threat or disadvantage) people with disabilities is always, in all circumstances, unacceptable.

40.6 There is a clear need for education of health workers (at all levels) to be aware of special needs/issues of disability and their individual and collective responsibility to accord respect and dignity to all people.

40.7 Where legal issues relate to disability there is a need for additional care in the collection/management/access of or to health-related data.

40.8 Issues of informed consent and recognition of capacity to make decisions are critical.

40.9 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 regardless of whether or not they are a person with a disability or disabilities.

40.10 All health care professionals, including those charged with the collection, maintenance and use of health-related data have the same obligations in the discharge of their responsibilities to people with disabilities as they do to any other individual, including all obligations and requirements under this document.

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

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

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

40.14 Persons with disabilities cannot be compelled to disclose their disability status or their health-related data relating to that disability. Where accreditation or certification of the fact of disability is needed to access a benefit or service by an individual, the certification of having a disability by an authority must be sufficient to establish entitlement. It is not lawful to require disclosure of all or part of the health-related data of that individual that relates to any assessment of disability, only the outcome may be required.

40.15 Particular care in the collection and management of health-related data must be taken. Inaccurate or inadequate health-related data concerning disability may result in adverse outcomes including, but not limited to, denial of or reductions in health and related services.

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

40.17 All health service providers must treat individuals without discrimination on the basis of disability status.

40.18 Access to the health-related data of individuals with a disability or disabilities must be in accord with the general principles of these Guidelines and must be dealt with on the basis of serving the interests of the subject individual. That interest must not be subordinated to the claimed interest of the State or of any institution or entity. Access to health-related data and information relating to a decision to be made about the health care of a person with a disability or disabilities must be in a form that is accessible to the person living with a disability or disabilities prior to any decision being made.

40.19 A person or other entity making a decision concerning health-related data must do so in a way consistent with that person's gender, gender identity and expression. A person's right to confidentiality of information about their health-related data must be recognised. This includes health-related data about the disability status and disability or disabilities and individual is living with.

40.20 Programs of education and training are necessary to enable the implementation of these provisions with full respect for people with disabilities in the collection, retention and other uses of their health-related data.

Chapter XXI. Gender and Health-related data

41. Gender and Health-related data

40.1 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 regardless of their gender, gender identity or expression.

40.2 It is a fundamental principle that regardless of gender, gender identity or expression, individuals are entitled to a level of health care equivalent to that provided to anyone else in their wider community. All health care professionals, including those charged with the collection, maintenance and use of health-related data have the same obligations in the discharge of their responsibilities to such individuals as they do to any other individual.

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

40.4 Health-related data concerning gender, gender identity and expression, is sensitive information. Particular care is needed in relation to its management. For some individuals, the collection of health-related data concerning gender, gender identity and expression is of even greater sensitivity.

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

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

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

40.8 Health practitioners, administrators and those engaged in provision of health services, 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 health-related information relevant to their health care needs including that relevant to their gender and gender identity, as well as to their own health records, and that this access is treated with confidentiality.

40.9 Particular care in the collection and management of health data must be taken including the categories used as gender markers. Inaccurate or inadequate identity data arising in health sector documents may result in adverse outcomes including, but not limited to, denial of or reductions in health and related services.

40.10 Individuals of diverse gender identity and expression are particularly vulnerable to human rights violations when their name, sex and gender details in official documents do not match their gender identity or expression. All necessary measures are to be taken to ensure that systems, procedures and data collection exist to reflect the person's self-defined gender identity. Those responsible for the collection of health data relevant to individuals in a gender change transition, should be particularly alert to the necessity to record such changes.

40.11 All health service providers must treat individuals and their partners without discrimination on the basis of gender, gender identity or expression, including with regard to partner recognition in systems, procedures and data collection, for example, as 'next of kin'.

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

40.13 A person or other entity making a decision concerning the health-related data of a person must do so in a way consistent with that person's gender, gender identity and expression. A person's right to confidentiality of information about their health-related data must be recognised. This includes health-related data about the gender, gender identity and gender expression of the person.

40.14 Health workers often lack basic information or training about specific health related data management requirements and concerns relating to gender, gender identity or expression. Programs of education and training for all involved in delivering relevant health care are necessary to enable the implementation of the provisions of this Guideline with full respect for each person's gender, gender identity or expression in the collection, retention and other uses of their health-related data.

40.15 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 accord with the provisions outlined in Chapters II and III, and with ethical consideration of advising the person concerned, while providing suitable and specific measures to safeguard their rights and freedoms.

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

Chapter XXII. Intersectionality and Health-related data

42. Intersectionality and Health-related data

41
42.1 The Recommendation in Sections 36, 39, 40 and 41 addresses special protection of health-related data of individuals as part of a social group.

42.2 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.

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

42.4 It is fundamental to acknowledge the intersectionality of different factors attributed to individuals to guarantee that the level of protection of their health-related data is the same. Regardless of the social group an individual is part to, every individual should be provided with the same standards in the health-care sector.

42.5 Intersectionality should be considered throughout all stages necessary to achieve the highest and equal protection of health-related data, including policy and law making.

42.6 Awareness of intersectionality as it applies to both healthcare professionals and to individuals in their care, is an important component of training in the standards applying to health-related data.

References

43. Bibliography

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Sullivan, Hannah R., *et al.,* Are Current Tort Liability Doctrines Adequate for Addressing Injury Caused by AI?, AMA Journal of Ethics, February 2019, Volume 21, Number 2:E160-166

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

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