[Place], [Date] [REFERENCE]

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

Mandate of the United Nations Special Rapporteur on the Right to Privacy – Task Force on Privacy and the protection of Health 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 February 2019 include Teki Akuetteh Falconer, Heidi Beate Bentzen, Elizabeth Coombs, Kenneth W. Goodman, Trix Mulder, Chris Puplick, *William Smart, Sam Smith, Jane Kaye, Steve Steffensen, Thomas Trezise, Melania Tudorica and Helen Wallace.*

This document is Version 0.1 and is work-in-progress. [1] It is known to be incomplete in a number of areas and is not intended to be considered as a finished document. In particular, 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 in this document provide further information on where in particular one or more members of the Task Force see room for debate. Additional input is needed and requested in all areas of the document.

The document does not reflect necessarily the view of the Taskforce on Health Data, nor does it represent the view of any individual member or groups of members of that Taskforce. This very early version is being released for consultation in order to provide the opportunity for everybody to comment on the document and contribute to its development.

[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

The purpose of this recommendation is to provide guidance by enumerating 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.

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 both the public and private sectors. It applies to the collection, storage, processing, analysis, exchange, transmission, and sharing of health-related data, including by means of digital or other technologies.

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.

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. This recommendation applies to individuals, government departments, agencies and authorities that may engage in personal activities in connection with their employment, service provision, volunteer work or under any contract where that individual deals with health-related data on their own behalf or as an agent for a third party.

3. Definitions

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

- "anonymisation" means a process applied to personal data so that the data subjects can no longer be identified 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.
- "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, preservation, adaptation or alteration, retrieval, access, consultation, use, disclosure,

Kommentiert [A1]: Comment of a Task Force member (CTFM): There is a need to emphasize civil and political rights or put this in a broader human right context. A new wording will be provided by a taskforce member.

Kommentiert [A2]: CTFM: Clarification on a comment from a Taskforce member is pending: "Public Task"

Kommentiert [A3]: CTFM: The material scope of this Recommendation should be further clarified and specified. In particular, the second sentence of this 2.3 is problematic.

Kommentiert [A4]: CTFM: The definition of anonymization is contested. The issue to discuss is whether the data subject can no longer be identified. Proposals include to address the problem "no longer be identified" by:
a) Speaking of the degree of deidentification
b) Rewording"" the data subject is no longer identifiable"

Kommentiert [A5]: CTFM: The definition of controller in the part of "" has the decision making-power" could not be in line with some data protection laws. With the current wording, questions like whether *any* kind of decision making power is sufficient to render an entity a controller are raised.
An agreement on a definition of "controller" is needed.

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.

- "examination" includes any non-genetic or genetic test with 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).

- "external data hosting" means the use of third-party data service providers irrespective of the platform used to securely and permanently store data in a digital form or forms.

- "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.

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

- "health-care professionals" means all professionals recognised as such by law practising in the health, medical welfare or social welfare sector, bound by a confidentiality obligation and involved in providing health care.

- "health information system" means a system that provides the underpinnings for decision-making and has four key functions: data generation, compilation, analysis and synthesis, and communication and use. The health information system collects data from the health sector and other relevant sectors, analyses the data and ensures their overall quality, relevance and timeliness, and converts data into information for health-related decision-making[2].

- "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. Health-related data can be a basis for discrimination, and such discrimination may include "familial relationships" derived from health-related data.

- "health-related data breach" WORDING TO BE ADDED TO 'EXEMPT' intentional lawful destruction means the accidental, intentional or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, or prevention of lawful access to, or sale of, personal or health-related data transmitted, stored or otherwise processed;

Kommentiert [A6]: CTFM: Two open points in the definition:
(a)Should non-genetic info that reveals genetic info, such as family history be included in this definition?
(b) Should we specify if this definition includes somatic tumor mutation data which may not necessarily be considered acquired characteristic of an individual (but of the tumor). The existing definition has the advantage that it is already used in legal texts

Kommentiert [A7]: CTFM: Does the use of the term "social welfare sector" make the definition too broad? A professional from the social welfare sector would (probably) not be recognised as health-care professional by law

Kommentiert [A8]: CTFM: The scope of the definition is considered quite broad. There are two proposals to narrow the scope:
- clarify what sort of thigs do not count as health-related data
- include examples of information which could be treated as health-related data, e.g. taken from recital 35 GDPR.

Kommentiert [A9]: CTFM: The definition of "breach" is seen as problematic given that the "breach" is a term that is already in common use, which in a way does not include many of the wrongs in the definition of «health-related data breach»

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

- “indigenous data” refers to data information or knowledge, in any format or medium, which is about, from or may affect indigenous peoples or people of first nations either collectively or individually and may include the language, culture, environments or resources of indigenous peoples.

- “indigenous data 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.

- “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 whose health-related risks are covered by a contract, whether in the process of being drawn up or already concluded.

- “insurer” refers to both health-related insurance and re-insurance companies.

- “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.

- “mobile applications” means a set of means accessible in a mobile environment making it possible to communicate and manage health-related data remotely. It covers different forms such as connected medical objects and devices that may be used for diagnostic, treatment or wellbeing purposes.

- “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.

- “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 remain personal data.

- “recommendation” means this document.

Kommentiert [A10]: CTFM: These two definitions should include a reference to health.

Kommentiert [A11]: CTFM: there is a need to define “identifiable”.

- "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.

- “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.

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.

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 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. Security measures must take into consideration technological developments, the sensitive nature of health-related data and the assessment of potential risks. They must be established, implemented, documented, and regularly reviewed to prevent risks such as accidental or unauthorised access to, destruction, loss, use, unavailability, inaccessibility, modification, disclosure of health-related data or personal data, or any other health-related data breach.

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 deletion as provided for in paragraphs 11 and 12 of this recommendation.

Kommentiert [A12]: CTFM: There is a need to define these terms.

Kommentiert [A13]: CTFM: There is a concern on the scope of the the current wording of this principle, which may prevent the reuse of health-related. One suggestion to address this concern is to add the clarification started in Art 5 (1)b second sentence GDPR. A sentence like “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.” could therefore be added here. Another example is brought in 7.2.

Kommentiert [A14]: CTFM: There is a concern from taskforce members that the requirement of the data subject not being in a position to provide the data is quite restrictive and might bring practical limitations, such as research. Others stated that a practicability clause would lower the protection level in many cases.

Kommentiert [A15]: CTFM: this principle is too strict, and not practicable, e.g. it can be difficult to determine if data are adequate to a particular task before analysis.

h. Data subjects have a right to data portability. This means that where the data subject has provided the health-related data and the data processing is based on consent or on a contract to which the data subject is a party, 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.

4.2 Health-related data protection 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 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. Legitimate basis of data processing of health-related data

5.1 Data processing of health-related data is lawful if, and to the extent that, the data processing is carried out in accordance with the principles stated in this recommendation, there are legal safeguards, and the processing is necessary for any of the following reasons:

a. direct benefits to the data subject such as medical diagnosis, care, treatment, and convalescence of the data subject;

b. preventive medical purposes and purposes of medical diagnosis, administration of care or treatment, or management of health services by health-care professionals and those of the social and medico-social sector, subject to the conditions provided for by law;

c. reasons of public health, for example 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;

Kommentiert [A16]: CTFM: There are several open issues:
- scope of the right: a right to portability of a copy of the data or portability and removal of the data?
- in what form, the way it was provided or way it has now been processed and cleaned?
- what about costs involved?

Kommentiert [A17]: CTFM: There are concerns that the reference to non-health-care professionals is not accurate. There are open questions like, e.g. why do we assume that health-care professionals are the correct baseline?

Kommentiert [A18]: CTFM: There are some doubts about the use of the term “convalescence” in this recommendation

Kommentiert [A19]: CTFM: There are concerns on whether this legitimate basis should be limited to health-care professionals, since the processing of h-r data for management and admin purposes is not necessarily done by health-care professionals.

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 managing 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; and

j. reasons of substantial public interest, on the basis of law, which shall be proportionate to the aim pursued, respect the right to privacy and data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

5.2 Health-related data may only be processed if 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.

5.3 Data processing of health-related data may be undertaken by a data controller where the processing is necessary for the execution of a contract entered into by the data subject or on his or her behalf with a health professional subject to conditions defined by law that must include the obligation of secrecy. Any contract under this provision may not diminish or contravene the rights of the data subject under this recommendation or any other law.

5.4 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).

Kommentiert [A20]: CTFM: There are concerns that this reference to the "reasons to believe [..]" limits the scope of this legitimate basis, e.g. What if they do wish to avoid contact but there is a safety issue?

Kommentiert [A21]: CTFM: point out the following on this subpara.:
- that having the reference to consent in a separate subparagraph appears to make consent a necessary requirement. One suggestion is to add this as an alternative to the circumstances listed under 5.1.
- whether certain processing activities would not be permitted if the law is silent on the exceptions as mentioned in this para, e.g. would this provision prevent public health/epidemiologic research or surveillance in jurisdictions/countries in which the law is silent?

Kommentiert [A22]: CTFM: proposal to have a separate section on withdrawal of consent as many aspects should be carefully addressed, e.g. some forms of withdrawal may increase risk of reidentification through linking codes, how to proceed with already processed information.

Kommentiert [A23]: CTFM: there is a need to define "informed consent".
One proposal is to use only the term "consent" and define this by distinguishing consent to research participation from consent to data processing.

Information communicated by the data subject to her or his contacts on social media is not manifestly making data public.

6. Data concerning fetuses and children

6.1 Health-related data and genetic data concerning fetuses, including but not limited to data resulting from a prenatal diagnosis, preimplantation diagnostics, or from the identification of the genetic characteristics of such fetuses, must be protected to the same level as other health-related data.

6.2 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 ability of the minor to fully understand consequences of processing must be taken into consideration. Therefore, where the child is below the age to 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. Children have a right to withdraw health related data from any health information system when they reach the age of legal majority.

Alternate 6.2 (below) upon which Taskforce Members views are sought with the different wording highlighted in yellow:

6.2 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 minor, her or his ability to give her or his consent shall be subject to the national law. However, if national law requires the consent of the holder(s) of parental responsibility, the consent of such holders 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. Children have a right to withdraw health related data from any health information system when they reach the age of legal majority.

7. Genetic data

7.1 Data processing of genetic data may only be undertaken subject to appropriate safeguards and where it is either prescribed by law or on the basis of the consent 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.

Kommentiert [A24]: CTFM: There is no consensus on the usage of the terms "unborn children", "fetuses", "embryos". The term used will need to be defined, including the term "children".

Kommentiert [A25]: CTFM: Deletion of the term "informed" is suggested in order to avoid confusion.

Kommentiert [A26]: CTFM: There are many concerns on this para.:
1. Scope of the para., e.g. reading this para. in the context of the US kids who want to get vaccinated against their parents' wishes, may not be covered by either of the proposed wordings.
2. Use of "fully" in the context of "fully understand consequences of […]". One proposal is to replace it with "sufficient".
3. Children's ' right to withdraw the consent. Questions like how does the right to withdraw work with children, if parents validly consent can children then withdraw?
4. Cases where parental consent is exempt by law should be taken into consideration.

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.

7.3 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. These must be subject to appropriate procedural safeguards. Such genetic data may not be used to determine other characteristics that may be linked genetically, 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. In the absence of consent from the data subject, genetic data to be used for the purpose of a judicial procedure or investigation must be collected from the data subject and not from health-related data databases or biobanks that do not have a forensic purpose.

Kommentiert [A27]: CTFM: proposal to indicate the responsible person to judge this threshold?

7.4 Data processing of genetic data can be used 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. Genetic data held in biobanks and other health-related data databases may be accessed also for these purposes.

7.5 Existing predictive data resulting from genetic tests must not be processed for insurance (including 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.

7.6 The data subject is entitled to 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 doctor 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

Kommentiert [A28]: CTFM: There is a need to differentiate between health care and health research being problematic for realizing learning health systems.

8.1 Where health-related data are disclosed by one health-care professional to another health-care professional and they are not connected to the same entity, 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.

Kommentiert [A29]: CTFM: There are concerns regarding the scope of the term "not connected to the same entity", e.g. does this term include business associates or the parties to Data Sharing Agreements?

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 data processing of that health-related data. Any such processing may only be authorised under appropriate and proportionate criteria defined by law, in light of the type of test used and the particular risk concerned.

Kommentiert [A30]: CTFM: There is a concern that this scope of this exception is broader than the rule.

9.2 Access to health-related or genetic data 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.

9.3 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. Where anonymisation is not possible, the data must be destroyed.

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

Chapter III. The rights of the data subject

11. Transparency of processing

11.1 The controller must take appropriate measures to inform the data subject of the 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 purpose for which the health-related data are to be processed, and the legal basis for the data processing of that health-related data,
c) 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,
d) 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 must comply with the terms of this recommendation),
e) the possibility, if applicable, of objecting to the processing of her or his health-related data, in the conditions prescribed in paragraph 12.2,
f) 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,
g) 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,
h) 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,
i) information required about the risks of the intended data processing and remedies available in the event of a health-related data breach,
j) 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,
k) 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,
l) 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.

Kommentiert [A31]: CTFM: more guidance needs to be included in order to determine the meaning of "impossible to contact"

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 data processing of health-related data that concern 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 erase 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 personal situation. 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, they 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 Data subjects may obtain from the controller, subject to conditions prescribed by law, where the data processing of health-related data is performed by automatic means, information on the transmission - 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 put in place all necessary measures to ensure respect for the effective exercise of the rights of data subjects contained in this recommendation 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.

Kommentiert [A32]: CTFM: The scope of the right to erase (deletion) is contested. It seems by the current wording that everything can be deleted without any alternative.
The reading of one taskforce member is that the right to erase should be exercised as provided by law.

Kommentiert [A33]: CTFM: There is a suggestion to state that this is not a right without exceptions.

Kommentiert [A34]: CTFM: The scope of this provision is contested among taskforce members. Some taskforce members are in the view that this provision will forbid machine learning.

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[3]

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.

Kommentiert [A35]: CTFM: proposal to include in the text of this recommendation the distinction between 1) consent to research participation (based on human rights, e.g. the Charter art 1 and 3, and which is expressed for instance in the Declaration of Helsinki) and 2) a legal basis for processing of health data, which may, but does not need to, be consent.

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 risks to the data subject 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. 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 accordance with a law that determines it to be 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 especially include the obligation to put in place technical and organisational measures to ensure the respect for the principle of data minimisation, purpose limitation and specification, deletion, destruction, pseudonymisation and anonymisation of data at the earliest opportunity.

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 precise as possible with regard to:

Kommentiert [A36]: CTFM: The additional requirements imposed to the controller while carrying out scientific research are contested. If these requirements were to stay, some taskforce members suggest to use the term "reasonably" instead of "as precise as possible".

a) the nature of the envisaged scientific research, the possible choices that she or he may exercise as well as any relevant conditions governing the use of the health-related data, including recontact and feedback of results/findings;

[3] Considering orienting with World Medical Association *Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Subjects 1964 and as amended and updated.*

b) the conditions applicable to the storage of the health-related data, including access and possible communication policies;
c) the rights and safeguards provided for by law, and specifically of her or his right to refuse to participate in the 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; and
d) the identity and location and purpose of any disclosure of health-related data to be made under paragraph 15.8 of this recommendation. The data subject must be informed specifically of her or his right to refuse to participate in the scientific research and withdrawal of consent to take part on the scientific research in the same manner as paragraph 5.2 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) 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).

15.6 As it is not always possible to determine beforehand the purposes of different research projects at the time of the collection of data, data subjects should be able to express consent for certain areas of research or certain parts of research projects, to the extent allowed by the intended purpose, with due regard for recognised ethical standards. 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. In the absence of such consent, any health-related data retained must be anonymised after the death of the data subject.[4]

Kommentiert [A37]: CTFM: There are concerns raised about
a. a possible contradiction between this provision and the purpose limitation principle; enabling that consent is given broadly for certain research areas,
b. need to define “certain areas of research.”

15.7 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) which includes lay members, prior to the commencement of the scientific research. This assessment must include consideration of the impact on data subjects in terms of privacy and other rights that may be affected. These assessments are to be reviewed periodically by the competent supervisory authority to ensure compliance with the terms of the approval, and the fact of the approval.

15.8 Health-care professionals entitled to carry out their own medical research and scientists in other disciplines may process health-related data as long as the data subject has been informed of this possibility beforehand in compliance with paragraph 15.4 and has consented to it.

15.9 Scientists holding health-related data will be liable for any health-related data breach in respect of the health-related data while it is in their possession or control. Complementary

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

safeguards determined by law such as requiring explicit consent or the assessment of the competent body designated by law must be established before other scientists may acquire health-related data.

15.10 Where scientific research purposes allow, health-related data must be anonymised. Where research purposes do not allow anonymisation, 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. This must be done where the purposes of the scientific research can be fulfilled by further data processing of health-related data that does not permit or no longer permits the identification of data subjects.

15.11 Where a data subject withdraws consent for scientific research, her or his health-related data processed in the course of that 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 manipulation 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 of her or his health-related data, this must be complied with.

Kommentiert [A38]: CTFM: It is contested if the data that was processed and analysed while there was a lawful basis for doing so, must also be destroyed

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

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

b. where law permits such publication on the condition that this is indispensable for the presentation of research findings on contemporary events 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.

Kommentiert [A39]: CTFM: It is contested. Genetic data is often impossible to anonymize, and the data sets are often huge. If one individual withdraws consent after the study has been published, should the article be withdrawn?

15.13 Provision(s) on transnational research to be drafted.

Chapter VI. Mobile applications

16. Mobile applications

16.1 Where the data collected by mobile applications, whether implanted on the individual or not, may reveal information on the physical or mental state of an individual in connexion with her or his health or concern any information regarding health care and medico-social provision, 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 and the software distributor 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.

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 flows of health-related data

17. Protecting health-related data flows

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

a. the data subject has given explicit, specific and free consent to the transfer, after being informed of risks arising in the absence of appropriate safeguards in a similar manner to paragraph 5.2; or
b. the specific interests of the data subject require it in the particular case; or
c. prevailing legitimate interests, in particular important public interests, are provided for by law and such transfer constitutes a necessary and proportionate measure; or
d. the transfer constitutes a necessary and proportionate measure for freedom of expression.

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, legal and all other applicable requirements by all health-care professionals and any person dealing with EHR systems.

18.2 No individual can be compelled to have an EHR against their will. Treatment of individuals cannot be withheld by virtue of the individual not having an EHR. No individual may be compelled to continue to have an EHR and where an individual provides notice that she or he no longer wishes to have an EHR, the health-related data in the EHR must be destroyed or rendered inaccessible to users of the EHR as soon as practicable after the instruction has been communicated. 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.

18.3 Data processing of health-related data in an EHR must be governed by an incremental system of “opt-in” requirements for the data subject to approve as they see fit having had the requirements consequences of any decision explained to them. Mandatory information regarding disclosure, ability to opt out and how health related data is handled must be provided to data subjects.

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.

Kommentiert [A40]: CTFM: There are concerns that to obtain prior consent of the data subject could be too burdensome in practice.

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.

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, which is a health-related data breach.

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. Data processing of health-related data may be undertaken in relation to health-related data in an EHR where the data processing of health-related data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where the data processing of health-related data is undertaken by a health-care professional subject under law or rules to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

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 may only be used for other purposes in anonymised form.

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 insurance companies

19.1 Genetic data and biological samples 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 Genetic data kept for statistical purposes must be rendered and retained in anonymous form in which identification of the persons is no longer possible, including when used in conjunction with other available data sets.

19.3 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.

19.4 TO DRAFT a clause or clauses addressing employers who are self-insured and therefore acting as insurers. Also address degree to which employer can share information about a specific employee or general employee population with third party insurers for the purpose of risk and rate determination.

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

Kommentiert [A41]: CTFM: it should be wise to stratify and say do not consider genetic data unless a policy is above X level.

Kommentiert [A42]: CTFM: a definition of "predictive genetic tests" should be considered.

Chapter X. Health-related data and employers

26. Health-related data and employers

1
2
26.1 A controller of health-related data may include an employer[5], 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.

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.

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

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 staff members when a new procedure is introduced and made permanently available for staff members. 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.

[5] 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.

Chapter XI. Indigenous Data Sovereignty and Health-related data

Kommentiert [A43]: CTFM: proposal not to treat this issue in a separate chapter.

27. Indigenous Data Sovereignty and Health-related data

19
20
27.1 Indigenous peoples have the right to:

Kommentiert [A44]: CTFM: proposal to define this term.

(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 analysis 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

Kommentiert [A45]: CTFM: proposal to define this term.

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 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 consequential 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

25
26
29.1 The data subject shall have the right not to be subject to a 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 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 suitable 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 within 72 hours from becoming aware of a health data breach[6].

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 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 receive 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 recommendation or otherwise results in a health-related data breach.

31.5 Disciplinary law applicable to the health care professionals and other persons undertaking data processing of health-related data in EHR systems must be implemented to counteract infringements of this recommendation.

[6] 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.

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 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 a protected disclosure is not accepted, either by the competent supervisory authority or as otherwise provided herein, the individual can elect to publish the claims they wish to make, however they will remain liable for the consequences, including under this recommendation.

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, all parties to the transaction or event that gave rise to the breach are liable to the data subject jointly and severally for damages arising from the breach.

Kommentiert [A46]: CTFM: this is a matter that should be determined by tort law rules in each jurisdiction.

33.2 To be drafted. Liability for faulty algorithms.

Chapter XVIII. AI, Algorithmic transparency and Big Data

34. Algorithmic transparency and Monitoring Outcomes

25
26
34.1 To be drafted. Artificial Intelligence and health-related data

34.2 Check automated decision making, but is there enough in here about use of algorithms for purposes other than diagnosis?

34.3 To be drafted. Outcomes with outcomes monitoring and examination to identify and take action in respect of prejudice and discrimination arising from automated decisions.

34.4 To be drafted. Provisions on Big Data.

34.5 To be drafted. Lack of inclusion of minorities in health-related data sets and the effect of this on automated decisions.

34.6 To be drafted. Use of other data for health-related purposes without permission. For example, use of photographs taken of staff members and published on web sites to diagnose health conditions without permission.

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

35. Health-related data and law enforcement including forensic databases

27
35.1 To be drafted. Provisions on health-related data in a law enforcement context, including forensic databases, to be drafted. An area to examine specifically is the retention of health-related data beyond the purpose and the period of time for which it was collected.

35.2 To be drafted. Where data has been processed for a specific purpose without consent (for example, for the identification of a missing person, or during a criminal investigation), such data must not be used for scientific research except for the specific purpose of assessing the validity of the method used to achieve that purpose.

36. Health-related data and immigration

36.1 To be drafted. Access to health-related or genetic data for immigration purposes requires the free, specific, informed and explicit consent of the data subject and must be subject to adequate safeguards in law to protect the rights and interests of data subjects

36.2 To be drafted. Other provisions on health-related data and immigration to be drafted.

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

37
37.2
37.1 To be drafted. Provisions on health-related data in the context of individuals in prison, individuals living with mental health issues confined to institutions, and individuals in the care of the state, such as may be the case for orphans.

38. Health-related data and Marketing

38
38.2
38.1 To be drafted. Concerns the interaction of marketing data and health-related data, e.g., an individual's search history on a website and its correlation to their health-related data.

39. Health-related data and diminished capacity

39
39.2

39.1 To be drafted. Concerns issues raised by dementia or Alzheimer's and all ages in which the individual is mentally incapacitated. Are there any limits to health care proxy decisions and the degree to which advance directives include direction to HC data?

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

40. People living with disabilities and Health-related data

35
36
37
38
39
40
41
42
43
44
45
46
47
40.1 To be drafted.

Chapter XXI. Gender and Health-related data

41. Gender and Health-related data

41
41.1 To be drafted.

Chapter XXII. Intersectionality and Health-related data

42. Intersectionality and Health-related data

42
42.1 To be drafted.

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.

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.

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.