COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 26 March / mars 2018 T-PD(2018)11

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

(Convention 108)

DRAFT EXPLANATORY MEMORANDUM

on Recommendation CM/Rec(2018) of the Committee of Ministers to member States on the protection of health-related data

Directorate General of Human Rights and the Rule of Law

General comments on the Recommendation

1. The increased use of digital technology over the last few years has led to an outright "datafication" of our societies. Data are everywhere. They constitute a valuable raw material for the creation of new knowledge and are of global importance for the growth of many countries.

2. Increased computerisation of the professions means that these developments also concern the health sector, particularly activities relating to healthcare and prevention, life sciences research, health system management, and the growing involvement of patients, thus combining several aspects of informational self-determination.

3. Mobility and the development of connected medical devices and apparatus also contribute to the exponential growth of the volume of data produced, while the Big data phenomenon[1] simply reflects the specific features of processing large volumes of data and their demands with regard to rapid processing, the disparity of data and the creation of special value.

4. Health-related data therefore present unique challenges and a potential for creating value, whose delivery will depend on countries' ability to organise the development of an ecosystem facilitating their use while guaranteeing respect for privacy and the confidentiality of personal data.

5. States in fact face major challenges today, for which health data processing can and already does perform an essential role: these challenges relate to public health, the quality of care, medical transparency and democracy, efficiency of the health system in an overall context of growing health expenditure and innovation and growth in such varied and important fields as personal medicine, precision medicine and information technologies.

6. E-health, that is use of information and communication technologies in the health sector, is clearly a powerful impetus for quality, safety and efficiency of care, now clearly acknowledged by all stakeholders.

7. These multiple challenges differ considerably in comparison to 1997 when the Committee of Ministers of the Council of Europe adopted Recommendation (97) 5 of the Council of Europe on the protection of medical data.

8. Indeed, the increase in the use of ICTs in the health and medical welfare fields combined with the aforementioned challenges confronting our societies has had a systemic effect on organisations and on the role of all those concerned with medical care.

9. The need to exchange and share health-related data in the interests of better care

[1] Big data: the expression "Big data" normally refers to extremely voluminous sets of data which can be computer analysed so as to extract statistical inferences with regard to data patterns, trends and correlations. For further information, see the "Guidelines on the Protection of individuals with regard to the processing of personal data in a world of Big Data" https://rm.coe.int/16806ebe7a .

provision for individuals has become crucial and substantially alters the very nature of the relationship between carers and their charges, which, a few years ago, was still founded on a unique bond that was considered sacrosanct.

10. The increasing technical sophistication of multidisciplinary care means that a wide range and a growing number of players are involved in caring for individual patients. These processes result in increasing data flows, which consist either in data exchanges and sharing of data between players, reflecting the digitisation of correspondence and, based on the model of e-mail, enabling a player to transmit health-related data to one or more other players for a clearly identified purpose under a system of controlled distribution between the senders and the receivers of the data, or in making health-related data available, usually on a platform, so that they remain accessible, in accordance with specific rules, for purposes and persons not necessarily identified at the outset, along the lines of shared medical files.

11. It is crucial to point out that there is always a risk that health-related data which make it possible to identify a person may reveal intimate details of his or her private life and must, therefore, continue to have a special status and be protected by rules guaranteeing their confidentiality. Respect for professional (medical) secrecy is central to this guarantee.

12. The aim of the Recommendation is to help facilitate the full application of the principles of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 (ETS No. 108, hereinafter “Convention 108”) to this new environment in which health-related data are exchanged and shared.

Detailed comments on the Recommendation

Chapter I – General provisions

1. Purpose

13. Recommendation (2018)… is designed to take account of recent developments concerning health-related data: how can the exchange of digitised health data, which is necessary to improve the healthcare system and the care of individuals, be facilitated without undermining the fundamental principles of the protection of privacy?

14. The Recommendation sets out measures which ensure respect for the rights of individuals and the confidentiality of the health-related data being processed.

15. This new Recommendation obviously also takes account of the principles set out in Regulation (EU) 2016/6/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, such as the principle of privacy by design, which requires that account be taken of data protection from the design of data processing systems onwards and of the means of ensuring data portability through the interoperability of systems.

16. It also takes account of the outcome of the analysis of the questionnaires sent to Council of Europe member states prior to the launch of the revision of the 1997 Recommendation.

2. Scope

17. States are reminded that Article 6 of Convention 108 includes personal health data among the special categories of data which may only be processed if appropriate additional safeguards have been set up. It is therefore the responsibility of states to ensure that appropriate safeguards for the protection of persons are provided in cases where health-related data are processed.

18. Like the Convention, which draws no distinction between the public and private sectors, the Recommendation applies to health-related data processed in the context of activities in both sectors, including in the field of voluntary work, given that they must meet the same requirements and that there are frequent exchanges of data between the two sectors.

19. The scope of the Recommendation does not include data processing carried out at the initiative of an individual in a solely personal and domestic context. This is increasingly the case when using applications or connected devices in the domestic context and when such data are not collected by a third party but stored on devices in the home.

20. In this connection, it is important to point out that the application of data protection principles to commercial entities which provide services in the context of solely personal and domestic activities, using mobile applications involving the

processing of health-related data, could be the subject of a separate policy document, which would focus specifically on the implications of data processing in the mobile environment (in particular problems of cross-border data flows, which are not addressed in the Recommendation).

3. Definitions

21. The definition of the term “personal data” is that set out in Convention 108. It is a well-established definition, which has been reaffirmed over time in various legal instruments of the Council of Europe. The term “personal data” is broadly defined. It includes the routine use of new technologies and electronic means of communication in the health, medical welfare and welfare sectors.

22. “Data processing” begins with the collection of health-related data and includes all operations performed on data, whether totally or only partly automatic. Where no automated processing is used, data processing means one or more operations carried out on health-related data within a structured set of data which are accessible or can be retrieved according to specific criteria or which enable the controller or any other person to search for, combine or correlate data concerning a person.

23. The concepts of exchange and sharing of health data can now be features of health data processing.

24. Exchange is the communication of information to a clearly identified recipient or recipients by a known transmitting party. Use of a secured e-mailing facility is one example.

25. A distinction must be made between data exchange and data sharing, which makes information accessible according to a principle of permissions. Sharing allows information serving co-ordination and continuity of care, or the person’s interest, to be made available to several professionals entitled to be acquainted with it, without these persons necessarily being known at the outset.

26. The definition of “personal data” includes all information which may directly or indirectly identify an individual, thus taking into account pseudonymisation techniques, which now make it possible to “link up” information concerning one person without necessarily being aware of their identity.

27. The terms “anonymisation” and “pseudonymisation” refer to processes which are now commonly applied to health-related data, making it possible to either remove the link between the person’s identity and the data concerning him or her, or to “link up” information concerning that individual without being aware of their identity. The process of data anonymisation can be used to make it impossible to identify the person concerned directly or indirectly, although the risk of re-identification should be underlined given the correlations and inferences that can be made from several separate databases.

28. The definitions used are in keeping with those in the opinion of the Article 29

Working Party of 10 April 2014[2] on this subject.

29. Anonymisation (or disidentification) of personal data refers to the method applied to and the outcome of the processing of personal data so that the data subject can no longer be identified. Anonymisation is irreversible. Generally speaking, it is not enough to directly remove information which, in itself, identifies the individual to guarantee that it is no longer possible to identify the person. To be effective, anonymisation must prevent re-identification, which does not merely mean preventing individualisation (singling out an individual in a set of data, or finding a person's name and/or address) but also correlation (linking separate sets of data concerning an individual) and inference (inferring information about an individual from the set of data in question).

30. Pseudonymisation is a technique which consists in replacing in the data registered any identifying characteristic (usually a unique characteristic) by another. The outcome of the pseudonymisation may be independent of the initial value (as in the case of a random number generated by the data controller or a name chosen by the person concerned) or it may be derived from the original values of an identifying characteristic or set of identifying characteristics, for example by means of a hash function or a ciphering system. There is therefore always the possibility that the person may be indirectly identified. Pseudonymisation alone does not therefore make it possible to produce a set of anonymous data; it reduces the risk of linking a set of data to the original identity of the person concerned; it is therefore a useful security measure but not a method of anonymisation.

31. In terms of personal data protection, pseudonymised data remain personal data.

32. The proliferation of data from different sources relating to one individual, and the new capabilities for processing these data, especially "data mining", considerably alter the concept of reversibility of the anonymisation of personal data (re-identification). Data considered anonymous at a given time may later pose a high risk of re-identification as a result of the emergence of new techniques or of new data sources, particularly in the "Big Data" context. The safest anonymisation techniques remain data aggregation which transforms individual data into collective data. But these techniques preclude many subsequent processing operations. It is therefore often justifiable to preserve the individuality of data while containing the risk of re-identification of the subjects.

33. Anonymisation (an irreversible action) remains desirable wherever it is possible, and results in impersonal data. In all other cases, individual data must be considered pseudonymised (or indirectly name-specific) and pose a relatively high risk of re-identification on the one hand and of disclosure on the other. Appropriate security measures should result from an assessment of these two risks (re-identification and disclosure) having regard to the sensitivity of the data processed.

34. While respect for privacy and medical secrecy are two fundamental patient rights, all health professionals are bound by medical secrecy. But in order to ensure

[2] "Opinion 05/2014 on Anonymisation Techniques".

continuity of care or to determine the best possible provision of care, health professionals now need to exchange information on the patients of whom they take charge. This “shared secrecy” is generally recognised by law, which also defines its limits. The patient must, however, at all times be able to refuse the disclosure of information concerning him or her to one or more health professionals.

35. The term “health-related data” will henceforth be preferred to “medical data” so that the protective system can be applied to all processing of personal data relating to a person’s health and go beyond the scope of the medical professions, given that the sensitive data in question are increasingly used outside this environment.

36. It conveys a broader concept of health data, which today cannot be limited to the sole indication of an illness, since a person’s health care also entails knowledge of his/her family or social situation and involves a wide range of professionals in the health and welfare sectors. It includes the processing of information on the past, present and future, physical or mental health of a person, who may be sick or healthy.

37. Health-related data thus covers, in particular, all information relating to the identification of the patient in the care system or the means used for gathering and processing health data, all information obtained during a medical check-up or examination, including biological samples and genome data, all medical information such as an illness, a disability, a risk of illness, clinical, physiological or biomedical information or information concerning treatment, irrespective of its source, whether originating, for example, from a doctor or other health professional, a medical facility or in vivo or in vitro diagnostic testing.

38. This also concerns so-called medical welfare or welfare data, which refers to all data generated by professionals practising in the general welfare and medical welfare sector if they help to characterise the data subject’s state of health. For the sake of simplicity, the term health-related data also covers the term medical welfare data.

39. Health-related data should be defined more broadly so that the information characterising a person’s health situation as a whole is also afforded appropriate protection. Health provision for patients is now more comprehensive and must take account of a medical and social welfare dimension throughout their course of treatment. It must also incorporate all information concerning the person’s lifestyle and well-being where it is connected to his or her health.

40. “Genetic data” refers to all data pertaining to the hereditary characteristics of an individual or acquired during early prenatal development, resulting from the analysis of a biological sample of the individual in question: chromosomal, DNA or RNA analysis or analysis of any other element enabling equivalent information to be obtained.

41. “Controller” means the person or body with decision-making power over the purposes and methods of data processing, whether as a result of an official

appointment or of factual circumstances to be assessed on a case-by-case basis. For example, at a health establishment, the director is regarded as the controller. So as to determine whether persons or bodies may be regarded as controllers, particular attention should be paid as to whether they decide on the reasons for processing or, in other words, its purpose, along with the methods used. The decision to call on one service provider or another to help to set up the necessary tools for processing is the controller's responsibility. Other relevant factors in deciding on whether persons or bodied can be qualified as controllers include whether they have control over the processing methods, the choice of data to be processed and the persons authorised to access data. Persons who are not directly subordinate to the controller and carry out processing on his/her behalf in accordance with their instructions are called "processors". Controllers still have responsibility for processing where it is conducted on their behalf by a processor.

42. This concept should today take into account the absence of material boundaries to data transfers and the undeniable new responsibility of Internet platforms in processing data and, in particular, in determining the means used.

43. A "processor" is any natural or legal person (other than a controller's employees) who performs processing operations on behalf of a controller in accordance with his/her instructions, which set the limits on the authorised use of personal data by processors. Hosting a data base or carrying out maintenance activities on a controller's behalf are typical processing activities.

44. The definition of the term "reference frameworks" is justified by the growing importance of such frameworks in the development of health information systems and health-related data. Compliance with them creates the conditions for the interoperability of the systems without which the exchange and sharing of data are impossible, and also helps to enhance data security. Some reference frameworks serve as a basis for certification procedures, and compliance with them may be of such importance in specific areas that they can be made enforceable by national legislation.

45. Compliance with reference frameworks makes it possible to create a structured set of information, thereby constituting a common framework for all applications processing health data.

46. The term "mobile applications" is linked to the concept of mobile health, which has been developing for several years now in all countries (as demonstrated by the answers to the questionnaire). It corresponds specifically to the use of connected devices for health data management purposes. This development takes various forms and covers several categories of applications, which are themselves used for very different purposes. From medical systems to "m-health" or "quantified self" applications, it is necessary to lay down certain principles for the use and processing of health-related data by these connected devices, one of the major characteristics of which is to increase the quantity of data produced.

47. Traditionally it has been health care that produces data – a visit to a health professional provides information for a medical record. Henceforth, these new medical services, many of which, but not all, are available in a mobile situation,

will produce, via sensors and algorithms, data that will have an impact on care.

48. The definition of the term “health professionals” must refer in each country not only to a list of professions but also to lists of persons and the means of identifying them with certainty. The management of the identities of these professionals in the health and medical welfare sector must be performed in such a way that citizens can be sure that they will be cared for by a community of health-service providers bound by professional secrecy. This will also make it possible to provide the basis for allocation of means of authentication in the various information systems and to ensure traceability of access to health-related data.

49. The use of third-party organisations to ensure the secure and long-term outsourced storage of health-related data on the Internet has led to the introduction of “external hosting” of health-related data.

50. Outsourced hosting has now become an efficient way to manage databases and a necessary gateway for data exchange and sharing functions. The term cloud computing is used to define the different ways in which these databases are made available on the Internet: Saas (Software as a service), Iaas (Infrastructure as a service) and Paas (Platform as a service).

51. The sensitivity of the health-related data hosted on these platforms means that arrangements must be made to ensure a high level of security for the persons whose data are concerned.

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

4. Principles concerning data processing

52. It should be recalled that personal health-related data can only be processed in the cases determined by domestic law, and at all events in a manner respecting professional secrecy, the privacy of individuals and the confidentiality of this information.

53. The principles governing personal data protection as set out in Convention 108 must be observed. They should be highlighted as a general, mandatory framework and include a specific and legitimate aim of processing, relevant data, limited data storage time, introduction of security measures such as to guarantee the confidentiality of the data, and respect for the right of individuals and their information.

54. Member states may include stricter provisions in their domestic law providing more protection for data subjects, where it comes for instance to the processing of genetic data.

55. The principle of fair collection implies that health-related data should, under normal circumstances, be obtained from data subjects themselves. This principle therefore relates to the “disclosure” of these data by data subjects themselves, not to the “communication” of health-related data by third parties (health professionals).

56. Clearly, this rule cannot always be applied: in such cases, other sources of information may be consulted only if this is necessary to achieve the purpose for which the data were processed (medical treatment, for example) or if the data subject cannot supply the data himself/herself. However, at all events, collection of health-related data must comply with the other provisions of principle 5.

57. The rights of persons whose data are collected and processed must be respected, particularly their rights of access and objection to, and communication, rectification, erasure and portability of data.

58. At all events, it is still for the national data protection authorities to satisfy themselves that these principles are observed and to disseminate all recommendations calculated to ensure compliance with the “privacy by design” principle.

59. The principles of personal data protection should be taken into account and incorporated right from the design stage of the information systems processing personal health data. Compliance with these principles should be reviewed regularly throughout the processing life cycle. The data controller must assess the impact of the applications used in terms of data protection and respect for privacy.

60. The duty of data controllers to protected health-related data properly is linked to their responsibility to check and be in a position to demonstrate that the data processing is compatible with the law in force. Among the appropriate steps that controllers and processors may have to take to be in compliance are training of employees, establishing suitable notification procedures (indicating for example when data must be deleted from the system), drafting specific contractual clauses where processing is delegated, appointing data protection officials and setting up internal procedures for checks and demonstration of compliance.

61. In principle, only health professionals, bound by rules of confidentiality, should collect and process health-related data, or where necessary, persons acting on behalf of health professionals, as long as such persons are subject to the same rules.

5. Legitimate reasons for health-related data processing

62. In accordance with the principle of lawful processing, the requirements for legitimate processing must be clearly established and the circumstances in which health-related data may be processed must be listed for these purposes.

63. Health-related data may be processed if provided for by law, where there is a contractual obligation to do so, if the data subject has given his/her consent and, in any event, only if the safeguards outlined in principle 4 are respected.

64. Health-related data may be processed, if provided for by law, for preventive, diagnostic or therapeutic medical purposes, or the management of health services by health professionals, including those working in the social and medical welfare

sector.

65. Health-related data processed by a health-care professional for preventive medical purposes or for diagnostic or therapeutic purposes may, after the specific medical care, also be necessary to carry out other services in the patient's interest; for example, to provide the prescribed medicine, for the hospital's administrative staff to draw up invoicing documents, or even to arrange reimbursement of costs incurred by social security services. The authors of the recommendation felt that the purpose of processing by such "health services" (which does not cover insurance companies acting on a contractual basis) was compatible with the initial purpose of collecting health-related data, which was to administer care. Consequently, the processing of health-related data by these health services is allowed, provided that it is carried out in the patient's interest.

66. Such health-care services may be managed by the health professional who collected the health-related data or by someone else. In the latter case, the necessary health-related data may be passed on by the health professional in accordance with principle 9.

67. Health-related data may also be processed, if provided for by law, for public health reasons, such as protection with regard to health risks and health safety.

68. While it still seems necessary to list the various purposes for which health-related data may be collected and processed, account should also be taken of the fact that because of technological advances, the volume of data produced has increased and it is not always easy to identify their purposes in advance.

69. Traditional data protection principles are not always readily applicable to this "datafication" phenomenon, a practical example being big data. It therefore seems necessary to provide, alongside conventional purposes of health data processing, for states to be able to provide for uses of these data.

70. One example could be the possibility now afforded by big data to be able to identify public health problems that could not be known about before but which it is now possible to find out about through the analysis of a larger quantity of data produced for the purposes of individual care. It must be possible to process health-related data for purposes not initially provided for, although still compatible, while respecting the appropriate safeguards.

71. Where the law so provides, health-related data may be processed for the purpose of safeguarding the vital interests of the data subject or another person. There are cases in which consent cannot be obtained owing to an emergency or because of the patient's condition.

72. Health-related data may also be processed, where this is provided for by law, for reasons of public interest connected with the management of claims for social welfare and health insurance benefits and services. Because they cover the costs of health expenditure, health insurance bodies are required to process health-related data.

73. Health-related data may also be processed, when provided for by law, and under

the conditions established therein, for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes. Processing carried out by medical research institutes or for statistical purposes to assess the level of health of a population or the prevalence of diseases for epidemiological purposes form part of such purposes. The same can be said for clinical trials prior to the release of new molecules on the market.

74. Where the law so provides and with due regard for the relevant and appropriate safeguards, processing of health-related data must be possible to enable controllers to fulfil their obligations and exercise their rights or those of the data subject regarding employment and social protection. Occupational health services may collect and process the health-related data needed to assess whether staff are fit for work. Appropriate safeguards must, however, be established to prevent employers from receiving health-related data.

75. The processing of health-related data for the establishment, exercise or defence of a legal claim may be carried out only when a specific case occurs, for example a conflict between a doctor and a patient about treatment, allowing the doctor to communicate data to his/her lawyer in order to defend himself/herself in a lawsuit. Collection "in anticipation" is not lawful.

76. Health-related data may also be processed, where provided for by law, for reasons of substantial public interest. The monitoring of certain communicable infectious diseases may justify the compulsory collection of health data in the interest of public health.

77. Apart from any legal measure or obligation, health-related data may also be processed if the data subject - or his/her legal representative - has given consent, unless domestic law provides otherwise. The drafters of the recommendation were aware that, with regard to the protection of health-related data, consent of the data subject offers fewer guarantees than legal obligations or legal provisions which, under Article 6 of the Convention, must be accompanied by appropriate safeguards. In addition, the conditions for such consent and the possible exemptions are of great importance.

78. The matter at hand is consent to processing of health-related data, not consent to treatment which, subject to some exceptions, remains an incontrovertible requirement.

79. Consent must be purely the expression of agreement to the use, sharing and exchange of health-related data under assured conditions of security and with clear prior information.

80. The requirement for consent should not shield or exonerate the person responsible for obtaining it from compliance with security measures or from the effort to inform, which are currently the only true protection for individuals.

81. Efforts should not focus disproportionately on the act of obtaining this consent in whatever form, but on what it embodies by way of requirements. While consent is a legal safeguard, it is not necessarily an ethical guarantee.

82. It therefore needs to be established what form consent takes, how it is obtained and the cases in which it must be obtained. Where it is required, it must be free, specific, informed and explicit. It must be prior to and/or concomitant with the collection and recording of the information.

83. It must remain reversible and controlled by the data subject and, since it may now take a digital form, traceability of the accessing of health data constitutes the technical means of ensuring respect for the patient's rights and is an essential safeguard. It should be stressed that since consent may be expressed by electronic means, robust security and authentication measures need to be established.

84. If processing of health data relating to a legally incapacitated person who is incapable of free choice is contemplated, and domestic law does not authorise the data subject to act on his/her own behalf, consent will be required from the person with legal entitlement to act on the data subject's behalf or of an authority or any person or body provided for by law.

85. If a legally incapacitated person has been informed of the intention to process his/her health-related data, his/her wishes should be taken into account, unless domestic law provides otherwise.

86. Lastly, under principle 5 it is permitted to process health-related data if they are necessary for respecting contractual obligations (for example, the contract between a hospital and an industrial group tasked with hosting data, where the appropriate safeguards are established so that the data remain unchanged), on condition, however, that all the appropriate safeguards are in place. The authors of the recommendation considered that a contractual obligation or right should be able to give rise to processing of health-related data, as the data subject had already given his/her consent when the contract was entered into.