The Protection of Data Concerning Health in Europe

Mulder, Trix

Published in:
European Data Protection Law Review

DOI:
10.21552/edpl/2019/2/10

The Protection of Data Concerning Health in Europe

*Trix Mulder**

More and more, medical practitioners use modern technologies such as apps and wearables in their treatment plan. The GDPR defines these kinds of data as 'data concerning health'. However, also the term 'medical data' is being used. Furthermore, the Council of Europe uses terms such as 'personal health data' and 'medical welfare data'. Using all these different terms makes it difficult to understand what is protected by these terms and what is not. This article gives an historical overview of the evolution of the protection of data concerning health, which also leads to a discussion on the current broad definition and offers possible solutions for the use of (the term) 'data concerning health'.

Keywords: Data Concerning Health, GDPR, Data Protection, Council of Europe

I. Introduction

If 2018 proved one thing, it is that data protection is very much alive. Both the European Union (EU) and the Council of Europe updated their regulations on data protection, which dated back to the previous century. Both updates introduced numerous changes in the processing of personal data in general and as such also affected the field of health. Even before the development of Information and Communication Technologies (ICTs), the healthcare sector has used patient files. Nowadays, most of these patient files are digital. With the rise of ICTs, legal aspects of computing in the healthcare sector became an important factor.[1] For example, many questions arose on liability, the use of diagnosis systems by laymen and a patient's right to privacy.

Although the consolidation of ICTs as an information tool was not the first time questions on privacy were raised,[2] their introduction into our society did increase the interest in the topic of privacy in general. It may not have been technically feasible in the 70s and 80s, but in 2019 people are able to track almost all their activities using modern technologies such as apps and wearables. There are, for example, apps that track how much someone exercises during the day; other apps measure food intake and there are even apps which measure someone's heartrate and blood pressure. The arrival of wearables made self-tracking even easier.[3] People can use wearables to measure almost everything that happens without being consciously aware of it. In this manner, by wearing something that someone would have worn anyhow, for example a watch or even glasses in the near future, people can track their day-to-day life.[4]

Since people are able to measure so much about themselves in their daily lives, it is not surprising they would want to share this data with a practitioner when needed. This leads to the situation that data used by practitioners nowadays originates from different sources: from patient files and from data collected by patients themselves. The use of heterogeneous data sources breaks boundaries creating new information flows and risks for privacy.[5] It is,

DOI: 10.21552/edpl/2019/2/10

* Trix Mulder LLM, PhD Candidate at the Security, Technology and e-Privacy research group at the Faculty of Law at the University of Groningen. For correspondence: <t.mulder@step-rug.nl>.

1 RN Freed, 'Legal Aspects of Computer Use in Medicine' (1967) 4 LCP 674.

2 SD Warren and LD Brandeis, 'The Right to Privacy' (1890) 4 HLR 193; WH Taft and Supreme Court of the United States, 'U.S. Reports: Olmstead v. United States' (1927) 277 U.S. 438 <https://www.loc.gov/item/usrep277438/> accessed 1 March 2019.

3 B Mittelstadt, 'Ethics of the health-related internet of things: a narrative review' (2017) 19 EIT 157-175.

4 M Niezen, 'Baas in eigen lichaam' (2019) 11 De Groene Amsterdammer; eHealth, Wellbeing & Ageing Newsletter, 23 February 2017.

5 S Barocas and H Nissenbaum, 'Big Data's End Run around Anonymity and Consent' in L Julia et al (eds), *Privacy, Big Data and the Public Good* (Cambridge University Press 2014) 44–75.

however, the question whether the privacy of these data flows are sufficiently protected by the new legal framework of the General Data Protection Regulation (GDPR).[6]

The European Union replaced Directive 95/46/EC from 1995 with the GDPR while the Council of Europe modernised its Convention 108 from 1981.[7] Both legal instruments deal with the protection of personal data, both instruments have a special categories of personal data and both instruments believe that data that reveals information about someone's health status should be given extra protection and should therefore be part of the special categories of data. Where the GDRP uses the term 'data concerning health' the modernised version of Convention 108 does not use a definition but merely says that the processing of personal data for the information they reveal relating to health should only be allowed when appropriate safeguards are enshrined in law.[8] Therefore, the question is whether both legal instruments protect the same phenomena? And if so, why did they choose different wordings to protect the same thing? Using different terms for the same phenomena could make it harder for practitioners to decide whether or not they can and will use these data for their treatment of a patient. This is especially interesting since data protection law in Europe has already been labelled a 'dead letter' with regards the protection they offer for an individual in practice.[9]

This article answers the question why different terms are used in European data protection regulation to protect 'health data'. In developing an answer, attention is given to the origins of the protection of personal data in general and health data specifically. Giving such a historical overview of the evolution of the protection of personal data is indispensable to understand the choices made by both the EU and the Council of Europe in 2018. By looking back in time, it might be possible to learn from what happened in the past and to apply this knowledge on new technologies, for example apps and wearables. In any case, we will have better understanding of what is going on.

II. A Historical Overview of Health Data Protection in Europe

Before zooming in to health data, this section delves into the history of privacy and data protection in general in Europe. The legal acknowledgment of privacy as a human right can be traced back to the Universal Declaration of Human Rights (UDHR) of the United Nations (UN) in 1948.[10] Inspired by the example of the UDHR, the Council of Europe followed in 1950 with the adoption of the European Convention of Human Rights (ECHR).[11] Both regulations address the concept of 'privacy' but make no distinction between privacy in general and data protection. Moreover, the ECHR does not recognise data protection as a standalone right.[12] The European Union followed much later, in 2000, with their Charter of Fundamental Rights of the EU, in which they do recognise data protection as a standalone right.[13]

1. The Recognition of Sensitive Data by the Council of Europe

From the 1970s on it became clear to countries that new technologies will have an impact on the amount of personal data that can easily be processed.[14] The first European legislator to take action on this matter was the Council of Europe. The first legal instruments to make a distinction between different types of personal data are the Council of Europe's resolutions from 1973 and 1974 are.[15] These two resolutions dealt with the protection of the privacy of individu-

6 Regulation (EU) 2016/679 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, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1 ('GDPR').

7 Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data ('Modernised Convention 108').

8 GDPR, art 4(15) and Modernised Convention 108, art 6(1).

9 BJ Koops, 'The Trouble with European Data Protection Law' (2014) 4(4) IDPL 250 <https://doi.org/10.1093/idpl/ipu023>.

10 United Nations, Universal Declaration of Human Rights <https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf> accessed 1 March 2019.

11 RCA White and C Ovey, *The European Convention on Human Rights* (OUP 2010) 4.

12 J Kokott and C Sobotta, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the EctHR' (2013) 3(4) IDPL 222 <https://doi.org/10.1093/idpl/ipt017>.

13 art 7 of the Charter deals with the respect for private life, while art 8 protects personal data.

14 PM Regan, *Legislating Privacy. Technology, Social Values and Public Policy* (University of North Carolina Press 1995) 25.

15 Resolutions (73)22 and (74)29.

als in relation to electronic data banks in the private sector and the public sector, respectively.[16] Remarkably, the level of protection for sensitive data is not the same for both sectors. The annex from the private sector resolution mentions in the first article that '(...) in general, information relating to the intimate private life of persons (...) should not be recorded or, if recorded, should not be disseminated.' However, Article 3 of the Public Sector Resolution speaks about the processing of 'information relating to the intimate private life of individuals,' and sets several requirements for the processing of these types of data. The Private Sector Resolution states that sensitive information should not be recorded, or at the very least not be disseminated, whereas the resolution for the public sector only states that the existence of electronic data banks which process sensitive information must have been provided for by law and that specific law 'must clearly state the purpose of storage and use of such information.'[17]

One could ask which of the two resolutions established a higher level of protection with regards sensitive data. At first sight it seems that data controllers in the private sector were subject to stricter rules, since they could not record information on the intimate private life of persons, while the public sector could as long as they complied with the requirements. On the other hand, the private sector recommendation only proclaims that if information on the intimate private life of a person is recorded it should not be disseminated. We could than easily conclude that the Private Sector Resolution offered more room for manoeuvre than the public sector one, which prescribes a set of requirements for processing sensitive data. Maybe this is due to the fact that in the 1970s it would have been logical to believe that the public sector had more personal data than the private sector.[18] Anyhow, the regime for data relating to the 'intimate private life of individuals' was as of 1973/1974 stricter than for other kinds of personal data.

2. Regulation of the Concept of Medical Data and Data Concerning Health by the Council of Europe

Over the years, the Council of Europe drafted several legal instruments as regards the protection of data concerning health and medical data. 1981 was an important year in this regard, since the Council of Europe issued both the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[19], better known as Convention 108, and Recommendation (81)1 on regulations for automated medical data banks. Convention 108 was the first internationally binding instrument for data protection in Europe and ended the different regimes governing data processing in the public and the private sector.[20] Although recommendations are not binding, Recommendation 81(1) followed Convention 108's example and also combined the rules for the private and public sector.[21] This meant that after almost a decade, the private and public sectors were treated as equals again by the Council of Europe as of 1981.

a. Convention 108 before 2018 and the Concept of Data Concerning Health

As is traditionally the case in Europe, Convention 108 is a general data protection convention, and it maintains the special categories of data created by the earlier resolutions.[22] The original version of Convention 108 dealt with personal data in general and recognised a special category of data with a specific regime

16 There has been a lot of discussion on the application of data protection law to public and private actors. See for an interesting overview of this discussion: O Lynsky, *The Foundations of EU Data Protection Law* (OUP 2015) 14-30; A Newman, *Protectors of Privacy: regulating personal data in the global economy* (CUP 2008) 84-87.

17 Resolution (74)29, art 3 para b.

18 Traditionally there have been two approaches with regards to privacy protection via data protection legislation. Although both do not make the distinction between the private and the public sector as such, it is interesting to see these approaches. Firstly the 'sectoral approach' which is the way the US protects personal data. This approach only provides data protection in specific areas (eg the banking sector). Secondly the 'omnibus approach' which is more in line with the European way of data protection as of the 1980s. This approach is a more general approach of data protection in which it does not matter which sector processes the personal data. See for example: O Estadella-Yuste, 'The Draft Directive of the European Community regarding the Protection of Personal Data' (1992) 41(1) ICLQ 175 https://doi.org/10.1093/iclqaj/41.1.170.

19 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, European Treaty Series - No 108, Strasbourg, 28 January 1981.

20 Convention 108, art 3 para 1.

21 F Benoit-Rohmer and H Klebes, *Council of Europe Law – Towards a pan-European legal area* (CoE Press 2005) 22.

22 ibid 100; L Determann, 'Healthy Data Protection' (SSRN, 24 April 2019) <https://ssrn.com/abstract=3357990> accessed 13 June 2019.

for the processing of that kind of data. Personal data concerning health was part of that special category of data.[23] The Convention's explanatory report mentions that the term 'personal data concerning health' was studied carefully by the Committee of Experts on Data Protection for Recommendation (81)1.[24] Unfortunately, I did not manage to find the report of the Committee of Experts on Data Protection where this was, supposedly, said. There is, however, no mention of the term 'personal data concerning health' in Recommendation (81)1; neither in the recommendation itself, nor in the explanatory memorandum. Despite this, the explanatory report for Convention 108 does point out that 'personal data concerning health' includes:

> (...) information concerning the past, present and future, physical or mental health of an individual. The information may refer to a person who is sick, healthy or deceased. This category of data also covers those relating to abuse of alcohol or the taking of drugs.[25]

Here the Council of Europe chooses to protect information rather than data.

The consequence of this definition is that information may also refer to a person who is healthy at the moment, but has had health problems in the past or is likely to get health problems in the future. Moreover, information concerning past and future physical and mental health is included. Consequently, this means that if a practitioner uses data in a treatment plan this data is always data concerning health, irrespective of the source of the data. Furthermore, combining data sets can make data that does not appear to be data concerning health at first, still become data concerning health after all. For example, some health insurance companies could use data from their clients concerning, among other things, primetime television viewing and frequency of purchase of general apparel in order to predict individual risk levels.[26] Strictly speaking, that kind of data does not directly concern the health situation of people, but, according to the explanatory memorandum, it becomes data concerning health once it is used to predict a health risk in the future.[27] As with the protection given by Recommendation (81)1, this again leads to the situation that the data itself is not protected, only if the data is used to gain information on someone's health does it become data concerning health.

b. Recommendation (81)1 for Medical Data Banks and Its Explanatory Memorandum

Recommendation (81)1 for medical data banks applies according to its Article 1.1 to:

> (...) automated data banks set up for purposes of medical care, public health, management of medical or public health services or medical research, in which are stored medical data and, as the case may be, related social or administrative data pertaining to identified or identifiable individuals (automated medical data banks).[28]

These automated data banks are called 'medical data banks'. The explanatory memorandum clarifies that the scope of the recommendation concerns: 'medical data contained in medical records established in the context of the doctor-patient relationship or in health records established for other purposes.'[29] It seems we can draw the conclusion from this that medical data can be recorded in medical records, which are part of the doctor-patient relationship, but medical data can also be recorded in health records, which are not part of the doctor-patient relationship. This data is, however, still medical data and both medical records and health records are part of medical data banks.

The Recommendation furthermore makes a distinction between different kinds of data that could be processed in medical data banks. The reason for this is the fact that different kinds of people have access to the data. The distinction made is between (1) identifiers and data relating to the identity of persons, (2) administrative data, (3) medical data and (4) social data. Regarding medical data and social data, a remark was made that suggests that there is a distinction between 'objective' and 'subjective' data.[30] The

23 Convention 108, art 6.

24 Explanatory Report to Convention 108, Special categories of data, no 45.

25 ibid.

26 S Garla et al, 'What Do Your Consumer Habits Say About Your Health? Using Third-Party Data to Predict Individual Health Risk and Costs. Proceedings' (SAS Global Forum, 2013) <http://support.sas.com/resources/papers/proceedings13/170-2013.pdf> accessed 13 November 2018.

27 Another example: F Pasquale, 'Redescribing Health Privacy: the Importance of Information Policy' (2014) 103 HJHLP 127.

28 Recommendation (81)1, art 1.1.

29 Explanatory Memorandum Recommendation (81)1, Scope and purpose of the regulations, no 21.

30 Recommendation (81), art 4.2.

Recommendation itself does not give definitions of these four terms, nor of the terms 'objective' and 'subjective' data. The explanatory memorandum gives an explanation for some of these terms. According to the explanatory memorandum medical data includes: 'information concerning the past, present and future, physical or mental health of an individual, as well as related social or administrative information.'[31] It is not surprising that the given definition is not limited to the doctor-patient relationship, since the explanatory memorandum already stated that medical data can be both part of medical records and of health records.[32] What is surprising is that the definition states that social and administrative data are also elements of medical data, while in the Recommendation medical data was separated from administrative and social data. This is confusing, since now the question arises whether social and administrative data are part of medical data or whether they are not.

A few paragraphs later, the explanatory memorandum clarifies the terms 'objective' and 'subjective' medical and social data with examples. Temperature, blood group, treatment prescribed, social background and profession are mentioned as objective data, whereas probable diagnosis, likely development of the disease, behaviour and aptitudes are examples of subjective data.[33] Again, it seems that these examples are not limited to the doctor-patient relationship. Although the explanatory memorandum does not formally define the terms medical records and health records, it is clear that medical data can be part of both records and that medical records are used within the doctor-patient relationship, while health records are not.[34] There are however also non-medical records that contain medical data; the recommendation uses the examples of insurance or employment records, which are not covered by Recommendation (81)1.[35]

To sum it up: according to Recommendation (81)1 medical data can be part of three types of records: medical records, which are used within the doctor-patient relationship and are covered by Recommendation 81(1); health records, which are used outside the doctor-patient relationship and are covered by Recommendation (81)1; and finally non-medical records, which seem to be used outside the doctor-patient relationship and are not covered by Recommendation (81)1. What is, however, very confusing is that it is not clear which medical data is still part of health records, and which medical data is part of non-medical records; and thus what medical data is covered by Recommendation (81)1 and what medical data is not.

c. The Next Step in Protecting Medical Data: Recommendation (97)5

After 1981 several recommendations where adopted which dealt with the use of personal data in different types of files.[36] However, none of these recommendations dealt with medical data specifically. It was not until 1997 that the Committee of Ministers adopted Recommendation (97)5 on the Protection of Medical Data, which replaced Recommendation (81)1. This replacement was necessary, since progress was made in both medical science and information technology, a conclusion already drawn by the Council of Europe's Project Group on Data Protection in 1990.[37] In the preamble, the Committee of Ministers mentioned the increasing use of automated processing of medical data by information systems and signalled that this data is not only used for medical care, medical research, hospital management and public health, but is also used outside the health care sector. The general purpose of regulation should be to guarantee that medical data is used in a way that the data subject's privacy and dignity are respected mainly because the content of the medical files may harm the patient if it is used outside the doctor-patient relationship.[38]

Recommendation (97)5 for the first time gives a definition of the term 'medical data'. It is referred to as 'all personal data concerning the health of an individual (...) also data which have a clear and close link with health as well as to genetic data.'[39] This

31 ibid no 21.

32 ibid and Explanatory Memorandum Recommendation (81)1, Introduction, no 3.

33 Explanatory Memorandum Recommendation (81)1, Recording of data, no 35.

34 ibid no 21.

35 Explanatory Memorandum Recommendation (81)1, Scope and purpose of the regulations, no 23.

36 eg Recommendation (83)10 on scientific research and statistics, Recommendation (89)2 on employment records, Recommendation (90)19 on payment, Recommendation (95)4 on telecommunication services and Recommendation (99)5 on privacy on the Internet.

37 Explanatory Memorandum Recommendation (97)5, Introduction, no 13.

38 Explanatory Memorandum Recommendation (97)5, Introduction, nos 9 and 10.

39 Recommendation (97)5, art 1.

again leads to the situation that medical data does not seem to be limited to the doctor-patient relationship, since it is 'all personal data concerning the health of an individual.' The Recommendation applies to anybody who processes medical data automatically, whether this is done routinely or occasionally and whether or not it is for a legitimate reason. This means the principles are applicable to the collection or the processing of medical data for the purpose of medical treatment, the assessment of the health situation or the fitness of a person, preventive care, health consultation, scientific research, rendering social assistance or reimbursement of insurance, as well as for the purpose of identifying an individual.[40]

The definition in Recommendation (97)5 is the most comprehensive definition possible, according to the explanatory memorandum. The drafters saw the need to go beyond the relationship between doctor and patient in order to cover any person likely to keep medical data.[41] In doing so, the Recommendation assumes that medical data goes beyond the doctor-patient relationship. Besides this, medical data also includes any information that can give an idea of an individual's medical situation, and Recommendation (97)5 mentions the examples of use for 'insurance purposes, such as personal behaviour, sexual lifestyle, general lifestyle, drug abuse, abuse of alcohol and nicotine and consumption of drugs.'[42]

d. A Comparison: Convention 108, Recommendation (81)1 and Recommendation (97)5

The Council of Europe issued two legal instruments in one year: Recommendation (81)1 and Convention 108. Recommendation (81)1 was replaced in 1997 by Recommendation (97)5. Even though Recommendations (81)1 and (97)5 only deal with medical data while Convention 108 deals with data protection in general, it might be interesting to compare the definition of data concerning health from the original version of Convention 108 with the definitions of medical data used in Recommendations (81)1 and (97)5.[43] Comparing these three definitions shows that they appear to be very much the same. On the other hand, this does not mean there is no distinction at all:

- Data concerning health in the original version of Convention 108:
  (...) information concerning the past, present and future, physical or mental health of an individual. The information may refer to a person who is sick, healthy or deceased. This category of data also covers those relating to abuse of alcohol or the taking of drugs.[44]
- Medical data in Recommendation (81)1:
  information concerning the past, present and future, physical or mental health of an individual, as well as related social or administrative information.
- Medical data in Recommendation (97)5:
  all personal data concerning the health of an individual (...) also data which have a clear and close link with health as well as to genetic data.

Firstly, comparing the definitions of 'medical data' from the Recommendations of 1981 and 1997 to the description given in by the Convention in 1981 to 'data concerning health' reveals some rather interesting changes. As we can see, in Recommendation (81)1 the term 'information' was used, which was in line with the previous recommendations and the ECHR.[45] However, in 1997 the definition does not use the term 'information' but used the term 'data' instead. One could think that the two terms are interchangeable, but it is question whether this indeed is the case, since only if data are interpreted it leads to information.[46] This means that as of 1997 data concerning the health of an individual was protected even without it being information yet. The protection of data is in this situation not depending on how the data is used, but on the content of the data itself, whether it is being used to gather information on someone's health or not. This does make sense, since it might be easier to enforce if the data itself is protected rather than making protection depended on how the data is used.

40 Explanatory Memorandum Recommendation (97)5, Scope, nos 60 and 61.

41 Explanatory Memorandum Recommendation (97)5, Definitions, no 37.

42 Explanatory Memorandum Recommendation (97)5, Definitions, no 38.

43 As stated in the opening paragraph of this section, the modernised version of Convention 108 does not use the term 'data concerning health'. This is why the modernised version is not used in this comparison and why it will be discussed in the next section.

44 Explanatory Report to Convention 108, Special categories of data, no 45.

45 See Resolutions (73)22 and (74)29 and ECHR, art 8.

46 Eg RL Ackoff, *Ackoff's Best* (John Wiley & Sons 1999) 170; M Kanehisa et al, 'Data, information, knowledge and principle: back to metabolism in KEGG' (2014) 42 (D1) Nucleic Acids Research <https://doi.org/10.1093/nar/gkt1076>.

Since Recommendation (97)5 is still in effect today, we can conclude that the term medical data is also applicable outside the doctor-patient relationship.[47] The explanatory memorandum of Recommendation (97)5 also mentions that principles of the recommendation are applicable to 'the assessment of the health situation or the fitness of a person, [and] preventive care (...)'[48] Projecting this description on the current situation of self-measuring via data provided by apps and wearables, one could believe that such data also should qualify as medical data and the processors of the data generated by the app maybe even as healthcare professionals.

However, this is not the opinion of the EU's European Data Protection Board (EDPB).[49] They described the term medical data in 2015 as being part of health data but believe that medical data is only the data on the health status of an individual when it is generated in a professional, medical context.[50] This seems logical, since this definition of the term medical data is consistent with the way the term is used in general language, although it is not in line with the definition used by the Council of Europe. The conclusion then is that the European Union and the Council of Europe work with different definitions of the same term, although the EU does not use the term medical data in their legislated instruments, they use 'data concerning health'.

Interestingly enough, the term data concerning health used in Convention 108 applies to 'information concerning the past, present and future (...).' This means that, according to the Council of Europe, there is indeed a difference between the scope of protection given by the term data concerning health, which offers protection in cases where data leads to information, and the scope of protection given by the term medical data, where the data itself is protected apart from the fact whether this data leads to information on a person's health.

The question is what this distinction between information and data entails for the protection of data concerning health and medical data in practice. If, for example, someone had a stroke and uses an app with pictures for groceries to help him improve his self-reliance, this data is not being labelled as medical data nor as data concerning health since this data does not have a close link to health nor does it lead to information on someone's health. However, if a physician uses this data to monitor the health progress of a person, it might still not be medical data but it becomes, according to the definition of Convention 108, data concerning health. From a data protection point of view this leads to the strange conclusion that, according to the Council of Europe, in some cases a doctor deals with data concerning health, while at the same time this data is not medical data. Time to find out how the European Union deals with this.[51]

3. The EU's Directive 95/46/EC and the Term 'Data Concerning Health'

Although one-third of the European Community did not adopt national privacy rules, despite the Council of Europe's Convention 108, the European Union did not act on calls for supranational action regarding data protection laws.[52] The European Commission did acknowledge that data protection was a necessary part of the protection of an individual and therefore encourages Member States to sign Convention 108. However, the European Commission did not see any reason at first to take action themselves. They were of the opinion that Convention 108 was an appropriate legal instrument to create a uniform level of data protection in Europe.[53] However, by the end of the 1980s the debate on the topic of data protection in Europe changed and in 1992 the European Commission presented the first draft of the new European Privacy Directive.[54] Still, there are opinions that the purpose of this Directive was not to provide data protection rules, but rather 'to ensure harmonisation of those rules so as to avoid any interference with the internal market.'[55]

47 The Council of Europe is currently working on an update of Recommendation (97)5, the report for this update will be discussed in para 4 of this article.

48 Explanatory memorandum Recommendation (97) 5, Scope, no 62.

49 Previously known as the Article 29 Working Party (A29WP).

50 A29WP, 'Annex by letter – health data in apps and device' (2015) 2.

51 Officially the regulation of the European Union only uses the term 'data concerning health', but explanatory documents also use the term 'medical data' to explain 'data concerning health'.

52 AL Newman, *Protectors of Privacy. Regulating Personal Data in the Global Economy* (CUP 2008) 84-85.

53 Commission Recommendation [1981] OJ L 246/31.

54 no 53, 91.

55 D Kelleher and K Murray, *EU Data Protection Law* (Bloomsbury Professional 2018) 4.

In 1995 Directive 95/46/EC came into effect. This Directive uses the term 'data concerning health'. Article 8 of the Directive labelled 'data concerning health' as a special category of data. As we saw in the previous paragraph, this is comparable to the Council of Europe's position on this matter. The Directive prohibited the processing of sensitive data, unless the exceptions in paragraphs 2 or 3 of Article 8 are met. One of those requirements, which is interesting in light of this paper, applies to processing that is necessary for purposes of preventive medicine, medical diagnosis, the provision of care or treatment, or the management of healthcare services.[56] The *Handbook on European Data Protection Law* describes these kinds of data as 'medical data'.[57] This description of medical data is the clearest description given yet, although it is not an official legal term in the Directive. Under the Directive, medical data seemed to be related to data in the doctor-patient relationship only and seemed to include data that is not medical data but is used by a doctor in a treatment plan. This makes the definition of medical data under Directive 95/46/EC clearer than the definitions given by the Council of Europe. In contrast, it is not yet clear what was covered by 'data concerning health' in the Directive.

In the original proposal for the Directive,[58] 'data concerning health' included 'information on [someone's] past, present and future state of physical and mental health and information on drug and alcohol abuse.'[59] This description does not seem to be limited due to the use of the word *included* and it matched the description used by the Council of Europe in Convention 108. Therefore, it can be concluded that medical data, according to the EU, is a specific category of data within the grander definition of 'data concerning health'.

It might seem that by defining the term 'data concerning health' as data that leads to information on someone's health, the offered protection is more limited as compared to the situation where the data itself is protected, regardless of whether it leads to information. However, it is the question whether this is true. For one thing, the term 'information' is a very broad term, which can lead to a very broad interpretation. This conclusion is supported by the judgment of the Court of Justice in the 2003 *Lindqvist* case.[60] Although the *Lindqvist* judgment was under the Directive, it is safe to presume that the same term 'data concerning health' used by the current the GDPR should also be interpreted broadly. The case dealt with the question whether 'the fact that an individual has injured her foot and is on half-time on medical grounds' constitutes as data concerning health under the Directive. The Court decided that this was indeed the case, given that a wide interpretation of this term was of importance in light of the purpose of the Directive.[61] The European Union updated Directive 95/46/EC and as of May 2018 the GDPR is in place.

III. The Current Picture: Data Concerning Health, (Personal) Health Data and Medical Welfare Data

The GDPR uses the term 'data concerning health', as did the Directive. In that respect, the European Union is consistent. However, to explain wat is covered by 'data concerning health' and 'medical data' other term such as 'personal health data' and 'medical welfare data' are being used. This section will examine these terms.

1. The GDPR and the Concept of Data Concerning Health

Data concerning health in the GDPR is part of the special categories of data. Article 4 paragraph 15 provides the definition of data concerning health in the GDPR; it may be the broadest definition yet, since it includes: 'personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.' The conclusion can be that this definition includes all the collected personal data, as soon as this personal data is used to gain information on the health status of a person. Therefore, it is very much the question whether or not personal data is considered to be sensitive data

56 GDPR, art 9 para 2(h).

57 European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law* (2014).

58 COM (90) 314 final.

59 ibid 36 and 62.

60 Case C-101/01 *Lindqvist* [2003] ECLI:EU:C:2003:596.

61 ibid paras 50 and 51; R Wong, 'Data Protection Online: Alternative Approaches to Sensitive Data?' (2007) 2(1) JICLT 10.

if it is not used to reveal information on someone's health. Malgieri and Comandé rightly wonder: '(...) should any data capable of (including very indirectly or with very complex data mining) revealing and individual's heath status be considered health data?'[62] Reading the definition in the GDPR the answer should be 'only if it is used for that'.

As stated in the preamble of the GDPR, data concerning health includes information on a disease, a disability and even a disease risk, independent of the source.[63] Although the examples mentioned in the preamble are all related to medical practice, the word *includes* makes it clear that this list is not limitative. This means that not only data collected from a source that is a medical device falls in the category of data concerning health, if the source is a non-medical device the data is also still part of the definition of data concerning health. This is also the conclusion of the Article 29 Working Party, now the EDPB.[64]

In 2015 the European Commission asked the Article 29 Working Party 'to clarify the scope of the definition of data concerning health in relation to lifestyle and wellbeing apps.'[65] The Working Party did so in an annex to the letter where they did not use the term 'data concerning health', but chose to use the term 'health data'. This leads to think that, according to the Working Party in 2015 health data and data concerning health meant the same thing. The Working Party also included the term 'medical data' in the description. It is their opinion that medical data is part of the broader category of health data. According to the Working Party, medical data is only generated in a professional, medical context,[66] whereas the definitions of medical data in the Council of Europe instruments seemed to be reaching beyond the doctor-patient relationship. The Working Party thus concludes that health data, a.k.a. data concerning health, is much broader than just medical data. For example, the Working Party analyses the term 'disease risk' mentioned in the proposal for the new GDPR, and eventually also included in the final version of the GDPR, as referring to data concerning the potential future health status of an individual. In their opinion this includes:

> (...) information about a person's obesity, high or low blood pressure, hereditary or genetic predisposition, excessive alcohol consumption, tobacco consumption or drug use or any other information where there is a scientifically proven or commonly perceived risk of disease in the future.

In other words, data which is not health data in itself can be qualified as such as soon as it is used to identify disease risks. This again makes the definition of health data context-dependent, since only personal data which reveals information on someone's health status is seen as data concerning health.

The example used by the Working Party are so called 'sad' message on social media, which are being used to determine if someone suffers from depression.[67] On the other side, the Working Party believes that data from an app that only measures how many steps someone takes and does not combine this data with other data on the data subject, if this data is not used in a medical context, the collected data cannot be categorised as data concerning health.[68] On an EU level it is thus important that the data is used to gain information on a person's health and it is irrelevant whether the data itself is related to a person's health. Here again it is the question whether this is enforceable in practice. Pasquale already suggested in 2014 that maybe 'the use of certain types of data in certain situations' should be prohibited.[69] This solution might have been interesting for the drafters of the GDPR. Of course, in that case, other question arise regarding how to limit and describe the situations, which are again open to interpretation. However, I do believe that looking at data concerning health in that way could solve most of the questions practitioners have regarding the use of commercial health apps and wearables in medical practice.

Interestingly enough, the definition of data concerning health in the GDPR does not mention that information concerning the past and future health of a person is also included, while this is explained that way both in the preamble and by the Article 29 Working Party. As we saw, the Article 29 Working Party decided to use the term 'health data' in their explanation, rather than using the GDPR-term 'data

62 G Malgieri and G Comandé, 'Sensitive-by-distance: quasi-health data in the algorithmic era' (2017) 26(3) I&CTL 229-249 <https://doi.org/10.1080/13600834.2017.1335468>.

63 GDPR, recital 35.

64 no 43.

65 European Commission, Letter of 5 February 2015.

66 no 43.

67 GDPR, art 4 para 15.

68 A29WP, 'Annex – health data in apps and devices' (2015) 3.

69 Pasquale (n 27).

concerning health'. On the one hand, this is logical since health data might be considered a simpler term for the same thing, but on the other hand it is confusing because why not use the term that is used in the GDPR, especially with the next chapter in mind, where we see other terms that are used to describe and distinguish from the terms 'medical data' and 'data concerning heath'.

2. (Personal) Health Data, Medical Welfare Data and the Position of the Council of Europe

Besides the terms 'medical data' and 'data concerning health' used in the context of the Council of Europe and the EU, the 2015 report for updating Recommendation (97)5 introduces an additional term: health data. As seen above, the Article 29 Working Party uses the same term in the same year. Where the Working Party uses the term 'health data' as a synonym for 'data concerning health', this is not the case for the Council of Europe.

a. Report for Updating Recommendation (97)5

What is striking at first is the statement that patients these days are active and wish to control their own treatment, data and data processing, even if they do not realise the full implications of this.[70] As stated in the introduction to this article, these days the data used for health treatment originates from different sources. Sometimes the source is a non-medical app or wearable that patients use themselves in order to measure their own health progress. Later in time, when the person becomes a patient, this patient might want to hand over this data to the practitioner in the hope that the information can help the recovery process. The update report starts with the statement that as of now, the term 'health data' will be preferred instead of 'medical data' and is defined as 'data capable of disclosing a person's state of health.'[71] The reason given by the report for changing the term from 'medical data' to 'health data' refers to the proposal of the European Parliament and the Council for the new GDPR in 2012. Strangely enough, looking at this proposal, the term 'health data' cannot be found. The proposal for the new GDPR uses the term 'data concerning health', not the term 'health data'.

The update report furthermore states that 'health data' is broader than 'medical data', since the concept of health data cannot be limited to the sole indication of a complaint, but is much broader than that. According to the report personal health data covers:

> all information relating to the identification of the patient in the care system or the device used for gathering and processing health data, all information obtained during a medical check or examination including biological samples and genome data, all medical information such as an illness, a disability, a risk of illness, a medical record, a clinical treatment or the physiological or biomedical condition of the person concerned, irrespective of its source, whether originating for example from a doctor or other health professional, a hospital, a medical facility or in vitro diagnostic testing.[72]

Then the report goes on and introduces a new term, medical welfare data. This is:

> all data generated by professionals practising in the general welfare and medical welfare sector, participating in the medical care of the person concerned by, for example, helping to characterise his/her state of health. For the sake of simplification, the term personal health data also covers the term medical welfare data.[73]

To summarise, the report for updating Recommendation (97)5 introduces two new terms: (personal) health data and medical welfare data. In the definitions we see that (personal) health data is the umbrella term, which also covers medical welfare data. I will first analyse the definitions of (personal) health data and medical welfare data, before moving on to the term used in the modernised version of Convention 108. What exactly do these concepts entail?

b. (Personal) Health Data and Medical Welfare Data

First, the term medical welfare data, since this term is part of the umbrella term (personal) health data.

70 Introductory report for updating Recommendation R(97)5 of the Council of Europe on the protection of medical data (2015) 3.

71 ibid 4.

72 ibid.

73 ibid.

It is important that medical welfare data is about data itself, since 'data' is used, not 'information'. Furthermore, it is clear that the term welfare data can only relate to data that is generated by professionals who practise general welfare and medical welfare. This leads to the conclusion that someone who is not a patient cannot generate this kind of data, since the main criterion is that a professional who practises general or medical welfare is generating the data.

It seems that the data has to be generated by the professionals themselves or at least in a setting where the professional is a part of generating the data. This seems to exclude data generated by patients themselves before seeing a professional. This suggests that if a patient generates data on their own, that data is not covered by term medical welfare data, even if the data is later used by a professional. It is the question whether the definition covers data that is generated by a patient after the practitioner has recommended the use of an app in the treatment process. From a legal point of view, this is not necessarily of real importance, since medical welfare data is also part of the term (personal) health data. This is why it is important to investigate the term (personal) health data before drawing any conclusions.

How does the term (personal) health data differ from the terms medical data and data concerning health? The definition shows that the (personal) health data covers all information that can identify the patient in the care system and also all information that is obtained during a medical check. The term medical check seems to relate to the doctor – patient relationship; otherwise the term 'health check' instead of 'medical check' would have been more logical.

Health data is related to 'information' instead of 'data' and all medical information is covered by the term and the examples mention, among other things, illness and the risk of illness. Especially the latter is of interest: for instance, information about the heart rate of patients can indicate a risk of illness. If you are about to get sick, your heart rate will be higher a couple of days before actually feeling sick. This means that even when someone measures his or her heart rate themselves (without a doctor's intervention), the resulting data would still be considered medical information. It is not necessary that this risk of illness is being determined by a doctor or that the device used is a medical device.

The latter can also be derived from the last part of the definition: irrespective of its source. If the source is a commercial app or wearable, it could still be medical information. It is, on the other hand, necessary that the heart rate is actually being used to indicate that someone is more likely to become sick, otherwise it would be medical data not medical information. Besides these questions of data protection, Mittelstadt justly notices that if commercial health apps are being used in a medical context, the practitioner has to be sure that the apps are scientifically reliable.[74]

Also covered by the term is information on a clinical treatment. This does not mean that the only the fact that you have been to the doctor, is already part of your (personal) health data. If, for instance, GPS information shows that someone visited a doctor, this data is only (personal) health data when it is used to draw the conclusion that this someone is indeed receiving treatment; because this newest term does not protect data, but information. Strangely enough, this is not the case for medical welfare data, where data is protected. This makes it very confusing to understand what is part of what.

Finally, in the modernised version of Convention 108 the Council of Europe did not use a term at all. There personal data, which is used for the information they reveal relating to health is labelled as a special categories of data. This kind of data can only be processed if appropriate safeguards are enshrined in law.[75] The draft explanatory report makes clear that this means that data itself is not protected, but only the use of this data, if this data is used to extract health information from.[76]

To conclude, it can be said that although the description of (personal) health data in the Report for updating Recommendation (97)5 from the Council of Europe differs from the description of the term data concerning health in the new GDPR, in substance they are the same. Both descriptions protect information on a patient's health, in a broad sense of the word, not data that does not lead to information. This is also in line with the modernised version of Convention 108, which chose not to use a term at all but simply protects data which is used to extract information on a person's health.

74 Mittelstadt (n 3).

75 Modernised Convention 108, art 6.

76 Draft Explanatory Report Modernised Convention 108, no 58, 10.

IV. Discussion

As seen above, the definition of data concerning health under the GDPR is the broadest definition yet. But even before the GDPR, several different terms were used to explain data concerning health or to elaborate on the term.

1. Use One Term: 'Data Concerning Health'

This article tried to find an answer to the question whether it is sensible to use different terms to explain the same concept, namely data concerning health. It turned out that the different terms overlap in definitions and make it even harder to understand what exactly is part of data concerning health and what not. It is therefore very much the question if introducing new terms helps to understand the concept of data concerning health. For example, whether medical data is used within the doctor-patient relationship or beyond that relationship, and whether such data can still be regarded as medical data or lifestyle data is not of importance from a data protection point of view. If the data can be categorised as data concerning health it is sensitive data and may not be processed according to the new GDPR unless the exceptions mentioned in the GDPR apply. Therefore, a clear definition of data concerning health will be very valuable.

2. Delineating the Use of Data Concerning Health

From the beginning, European legislators struggled with the definition of data concerning health. It was hard for them to determine what is covered by the definition and what is not. This, in turn, led to the situation that nothing was left out of the definition. Therefore, the current definition is so broad, especially in combination with modern technologies such as apps and wearables that it seems to cover almost all personal data, as soon as that data is used to gain information on someone's health.

Taking into consideration the fact that in some cases it depends how the personal data is used, before one can determine whether the personal data is considered to be data concerning health, it is very much the question whether a definition this broad can be enforced. Therefore, it might offer little to no protection in practice. What could be an interesting solution, however, is Pasquale's suggestion that 'the use of certain types of data in certain situations' should be prohibited.[77] According to him, data concerning health should not 'even enter the calculus of decision-making' in for example the employment and basic banking services.[78] Traditionally, the US have sector- and harm-specific laws, such as Health Insurance Portability and Accountability Act, while the EU traditionally has general data protection laws which apply to all sectors.[79] However, in my opinion, the solution offered by Pasquale can also be of interest for European data protection law. Especially, if this solutions is used in combination with the first solution: only use one term to describe 'data concerning health'. In that case, the definition of the term can be very broad, while it would still offer sufficient protection to people in practice.

3. A Way Forward

The EDPB feels that it is important that special measures are taken to protect data concerning health[80] and I agree with this. Data concerning health is sensitive data and therefore there should be restrictions for processing these kinds of data. However, to offer protection in practice it is important the provisions of the GDPR can be enforced. I therefore believe that we should start with (1) only use one term to describe data concerning health and (2) further discuss when data concerning health can be processed. In doing so, we do not have to delineate the current definition of data concerning health. Although I am aware that these two steps do not solve all the issues regarding the protection of data concerning health,[81] I do believe that if we are willing to address both these points, the protection of fundamental rights and freedoms of individuals regarding data concerning health might be one step closer.

77 Pasquale (n 27).

78 ibid 124.

79 Determann (n 22).

80 The EDPB uses the term 'health data' instead of 'data concerning health'.

81 There are, for example, also very important discussions on the concept of 'informed consent' and 'control solutions'.