BUNDESÄRZTEKAMMER

Bekanntmachungen

Statement

of the Central Ethics Committee at the German Medical Association

"Provision and use of treatment data for research purposes"[1]

In the event of any discrepancies between the English and German versions, the German version shall prevail.

Preface

The demand for efficient provision and use of treatment data for research is currently the focus of numerous initiatives at national, European and also international level. At the national level, however, implementation has so far been unclear and problematic – for example, in comparison to more digitised countries – due to a lack of common data standards, insufficient interoperability of documentation systems and, last but not least, restraints due to data protection regulations. Removing these constraints for the purpose of research reflects an important ethical desideratum.

At the same time, the use of treatment data for research purposes is in part subject to considerable concerns regarding informational self-determination as well as risks to the privacy of those providing the data. These aspects also require careful consideration in light of current events in Europe and the increasing sophistication of cybercrime. It is therefore also an important ethical desideratum to carefully weigh the opportunities and risks associated with data processing and to counterbalance them to the greatest extent possible with reasonable protective measures. The urgently needed socio-political debate has been neglected in recent years – also due to the pandemic. Therefore, great expectations rest on the draft of a law on the use of health data announced by the government coalition.

Within this context, in 2021 the Central Ethics Committee (ZEKO) set a goal to examine the implications of data-supported research particularly for the medical profession, in order to determine the potential of this research area and to counteract negative developments at an early stage. Such undesirable developments can arise, for example, if increased documentation requirements are at the expense of patient care. At the same time, the opinion emphasises the central role of the medical profession with regard to guaranteeing system trust and emphasises that this is essential for the success of data-based treatment research.

In order to do justice to the complexity and multidimensionality of the topic, ZEKO conducted a technical discussion with experts who are recognised in the field of research with treatment data in the run-up to the preparation of the Opinion. At this point, we would like to expressly thank the experts as well as the leaders and members of the work group for the careful preparation of the topic in the ZEKO. The many constructive contributions and the discussions characterised by mutual respect and trust have significantly strengthened the Opinion. Our sincere thanks are due to all those involved.

Berlin, February 2023

Prof. Dr. jur. Jochen Taupitz
Chairman of the Central Ethics Committee
at the German Medical Association

[1]The Central Ethics Committee discussed and adopted this Opinion in their session on 23.11.2022.
The Opinion is to be considered in the temporal context of its drafting and is based on the scientific findings and applicable legal provisions existing at that time.

Deutsches Ärzteblatt | DOI: 10.3238/arztebl.zeko_sn_behandlungs daten2022_en

1. Introduction

The progressive digitisation of the health care system also increasingly enables the use of health data generated in treatment contexts for medical research. The provision of treatment data for research is attributed to having great potential. It is intended to promote innovations in the diagnosis, therapy, prognosis, prediction and prevention of diseases, as well as to improve the performance of artificial intelligence (AI) systems developed for medical purposes by providing them with training data. Bold statements such as "data helps to heal" [1] or the talk of data resources as a "buried treasure that needs to be unearthed" [2] proactively highlight the opportunities of using already existing health data: advantages are seen, among other things, in the potentially highly effective and inexpensive implementation in research projects. In addition, it appears that treatment data are not only comparatively easy to obtain and available in large quantities, but that they also more closely reflect health care practice than data from clinical trials, which are generated in a highly standardised setting. The SARS-CoV-2 pandemic has particularly shown on the one hand how research results from the analysis of treatment data can contribute to better management of care.[2] It has also shown that the data required for this is not available in Germany to the necessary extent or in a timely manner as compared to other countries [3]. On the other hand, even data-intensive AI-based studies that were able to draw on very large data sets did not produce any diagnostic and therapeutic progress in the SARS-CoV-2 pandemic, which is attributed, among other things, to a lack of common data standards and insufficient data and study quality [4], but not lastly also to regulatory and administrative obstacles. The opportunities, however, are also offset by various risks, particularly with regard to the different purposes between research and treatment and the protection of patient privacy.

With regard to the use of treatment data for research purposes[3], several far-reaching (scientific) political processes have been initiated in Germany in recent years, which have significant consequences both for the future character of medical research and for clinical care. For example, the Federal Ministry of Education and Research (BMBF) funded the Medical Informatics Initiative (MII) with approximately 300 million euros from 2018 to 2022, a program in which the German university hospitals, together with other partners, plan to develop and implement strategies that improve the usability of data from patient care for research. The MII enables the exchange and use of data across locations by making clinical data available at participating hospitals and by creating the information technology requirements as well as an ethical-legal governance framework. Another relevant development results from the so-called "Patient Data Protection Act" (law for the protection of electronic patient data in the telematics infrastructure, PDSG), which will take effect in July 2024, and according to which insured persons are to have the option of releasing treatment data for research purposes via their electronic health record (ePA). According to the basic conditions regulated in § 363 SGB V, the decision for release as well as the selection of health data for release for research purposes is to be the responsibility of the insured persons, who voluntarily give their data for secondary use either to the research data centre (§ 363 par. 1–7) or directly to a research institution (§ 363 par. 8) based on informed consent.

But since developments in this area are extremely dynamic, the introduction of the opt-out model is already being discussed as an alternative to the previously proposed explicit consent (opt-in model)[4] with a view to the three different processes of creation, entry and use („all-in" or selected data sets with or without inclusion of sensitive data such as psychiatric diagnoses or HIV infection) on the one hand and the use of the data from the ePA for research on the other (see section 3.3.). The case is different with the "data transparency procedure" introduced with the Digital Health Care Act (DVG, 2019), in the context of which the pseudonymised[5] billing data of all 73 million people with statutory health insurance are brought together and transmitted to a research data centre (here, insured persons have no right of objection). Upon request, legally defined user groups receive access to anonymised data[6], and, depending on the research project, pseudonymised data for legally defined research purposes (§ 303a ff. SGB V).[7]

There are also requests from the European Commission to enable initiatives for the pooling and large-scale use of patient data. The European Data Governance Act aims, among other things, to promote the use of certain categories of highly sensitive data. It also talks about a concept of "data altruism" (voluntary provision of data by individuals or companies for the common good) and neutral data intermediaries[8] (see section 3.4.), which should increase trust in these services; an expert group called the "European Data Innovation Council" should regulate the further use of data subject to the rights of others [6]. The aim is to make the usability of treatment data from health care, which up to now have only been made available in aggregated form in the context of health services research, available to a large extent for research. Such a merger offers opportunities, but can also lead to tensions and conflicts. This is especially true because research and care are treated differently in ethics and law for good reason (see section 3.1.).

The proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space (EHDS Regulation), presented in May 2022, is intended to serve the further development of healthcare as well as research and development, primarily through improved secondary data use. Both the Data Governance Act and the Commission proposal for the EHDS are

[2] To improve the availability of data for COVID-19 and SARS-CoV-2, the Medical Informatics Initiative (MII) was supplemented by the Network University Medicine (NUM) and the embedded cohort platform "NAPKON". An overview of the projects completed under this initiative is available here: https://www.netzwerk-universitaetsmedizin.de/projekte/abgeschlossene-projekte (last access: 22.09.2022).

[3] In scientific discourse, reference is frequently made to the "secondary use" of "routine data". For the sake of clarity, this Opinion primarily addresses the provision of treatment data for research purposes.

[4] Opt-out only for the creation of an ePA means that it is made available to all insured persons, but its use is voluntary. There are different models for entering data in the ePA, e.g., "all-in" or selected data sets with or without inclusion of sensitive data such as psychiatric diagnoses or HIV infection. If an opt-out model were introduced for research, the health data would be available for secondary use without separate consent and the insured person would have to object to the release of data if they did not agree to secondary use.

[5] See section 4.1.

[6] See section 4.1.

[7] The Society for Civil Rights (GFF) is taking legal action against this regulation before the civil courts in Berlin and Frankfurt and is lobbying for a right of objection for particularly vulnerable people and better protection rights through encryption: https://www.medical-tribune.de/praxis-und-wirtschaft/praxismanagement/artikel/patientendatensammlung-risiko-einer-re-identifizierung-trifft-auch-aerztinnen-und-aerzten; https://www.heise.de/news/Richter-zweifelt-an-zentraler-Massenspeicherung-von-Gesundheitsdaten-7312977.html (last accessed: 16.11.2022).

[8] "In order to strengthen trust, trusted providers of data sharing services (so-called data intermediaries, e.g., data marketplaces) will consolidate and organise such data in a neutral manner. To guarantee this neutrality, the data intermediary must not share the data in his own interest (e.g., by selling it to another company or using this data himself to develop his own product) and must meet strict requirements to maintain this neutrality." [5].

designed as EU regulations and thus have direct legally binding effect.[9] Therefore, both regulations are also of immediate relevance for doctors.

Doctors are affected in several ways by the growing importance of the use of treatment data for research purposes:

a) In their role as caregivers, they increasingly have the task of informing patients about the possible usage of their treatment data for research, and supporting them in their decision-making.

b) Furthermore, it is already foreseeable that new requirements will be placed on the medical documentation of treatment processes so that these can be adequately recorded in terms of information technology and used rewardingly for research.

c) In their role as "data holders" (Art. 33 of the EHDS Regulation), practising physicians may have to store the data and make it available for requests of secondary use.

d) Researching physicians face the challenge of understanding the characteristics of treatment data-based research, exploiting its potential and appropriately addressing limitations. Part of this understanding includes research ethical issues such as informed consent, data protection and the social value of research with treatment data.

e) As recipients of research findings in the sense of "lifelong learning", doctors need a basic understanding of the specifics of research with treatment data in order to be able to appropriately interpret the significance of findings and integrate them into their clinical practice.

Aspects of research with treatment data can be found in both outpatient and inpatient care in distinctively characteristic ways. At least university hospitals are already largely familiar with the scientific use of treatment data, both in terms of personnel and material resources as well as in terms of the research competence of the doctors involved, or even document primarily therapeutic data in a dual function in the context of clinical studies. In outpatient (specialised) care, for example in radiology or human genetics, sometimes even larger disease-related patient collectives are cared for and correspondingly large data sets essential for research are generated. In most cases, however, this happens without the availability of research-relevant resources or special competences that go beyond the requirements of care. Especially in connection with so-called "widespread diseases" and with epidemiological questions, treatment data from outpatient care are of enormous scientific relevance. Unfortunately, there are hardly any research-related resources in this area compared to the generally scarce patient-related work capacities. Therefore, the qualitatively appropriate documentation of treatment data, which should also be secondarily applicable for research, requires special attention and support, especially in the sectors of medicine which are more remote from science. This refers both to methodological knowledge of new forms of data processing and to the structured logging of treatment data for transfer to research. Successful data-based research is also inconceivable without acceptance by both the professional actors and the patients concerned. Inadequacies in the practicability of the documentation systems, which result in multifaceted and bureaucratic requirements for the service providers, can lead to dissatisfaction on the part of both doctors and patients.

[9] Art. 288 of the Treaty on the Functioning of the European Union (TFEU).

The present Opinion is intended to provide an overview of the central issues of this complex topic, with a special focus on the role of physicians in outpatient and inpatient care. The opinion focuses on the release and use of treatment data, i.e., data that is generated in the course of regular patient care (in diagnostics and therapy). The release of other health-related data for research (such as billing or lifestyle data) is only discussed marginally. The Opinion is addressed to physicians and other health professionals, researchers, patient representatives as well as regulatory and politically active persons in the context of medical research.

2. Data work, data quality and a new approach to research

2.1. Data work

It sometimes appears that data from the medical treatment context is simply available and only needs to be compiled for research purposes. In fact, this underestimates the effort and processes that are necessary to make such data scientifically usable. In general, it should be noted that data are never "raw", but always already reflect certain contexts of their creation and collection (cf. [7]). This is why data are also referred to as socio-technical entities (cf. [8]). Data from the health sector are described overall as "very heterogeneous, ambiguous, noisy and incomplete" [9].

The use of aggregated data, for example for statistical analyses, machine learning (ML) or other forms of systematic processing, requires standardised collection of data in formats that are as uniform as possible. For this purpose, physicians or often also other health professionals usually have to enter these data into predefined software templates so that they can be collected in a structured form.[10] Structured data are, for example, diagnoses that are coded via ICD-10, prescriptions or laboratory tests. If data are not systematically coded and documented in a structured way according to other standards, but are only available in natural language as so-called free text, such as doctor's letters or anamnesis descriptions, they can only be made accessible using complex Natural Language Processing (NLP) procedures [10]. Despite great progress, this technology is not yet fully developed and has been afflicted by serious interpretation errors. These include the recognition of relationships between different entities or the temporal dimension of disease development for understanding past, present and future clinical events. Also, these programmes cannot use alternative sources of clinical knowledge (such as textbooks, automated diagnostic decision support systems) [10, 11].

Data work encompasses the processes required to transform treatment data created in the field into a usable resource for quality assurance, certification and other secondary purposes such as research applications (see section 2.2.). The increased documentation workload associated with this places new demands on physicians and other health professionals. The work is complex and demanding, and also requires cross-checking and double data entry to ensure data quality and achieve quality improvements. Knowledge of how to generate high-quality data in specific contexts should be considered early in the development

[10] This presentation is based on the assumption that various individual systems will continue to exist and data will therefore have to be entered twice or multiple times. It is also conceivable that a software system will be created in the future in which all data is bundled. With such a system, the expected documentation effort would be reduced. However, there will be additional challenges, among other things, due to the fact that the input can be optimised for different purposes and thus the information relevant to the treatment is no longer available in an optimal form.

Deutsches Ärzteblatt | DOI: 10.3238/arztebl.zeko_sn_behandlungs daten2022_en

of integrated systems within organisations [12]. A number of authors [13, 14] therefore call for this skilled but largely invisible work to be recognised and provisions to be made for its appropriate valuation. The interface between care on the one hand and research on the other also raises the question of who should make the corresponding investments and permanently incurred costs. It does not seem appropriate to place this burden unilaterally on the service providers.

In a multi-centre study that examined the documentation workload for quality assurance of tumour therapy using the example of primary operable breast carcinoma from initial diagnosis to completion of follow-up care, far more than 200 individual pieces of information had to be documented for one patient [15]. The time required was significantly higher in certified centres than in non-certified centres, and came to an average of about 23 hours across all centres. 40 % of the time required and 57 % of the documentation costs were accounted for by the medical profession, the rest by other professional groups ("study nurses", coding specialists, physiotherapists, psychologists, nursing staff, medical assistants, secretaries, medical-technical assistants, social workers).

In the process, data from the treatment context is often requested, which has already been documented by the treating physicians in other documentation systems, but is not yet available in a structured form. A recent study reports that physicians fear the effort involved and reject this type of effort "because no new data is generated, but existing information must be documented again" [16].

Currently, the additional effort of documentation lies mainly with the service providers. Consequently, data entry in the ePA is usually to be carried out by the physicians in addition to the primary documentation of the treatment. Special Medical Information Objects (MIO), which are new standardised data structures, have been developed for the structured recording of data in the ePA. These are used to document medical data – for example in an ePA – according to a defined, uniform format that can be read and processed equally by different systems, thus ensuring exchange between the individual actors. So far, for example, an electronic MIO model has been defined for the vaccination certificate, the dental bonus booklet, the children's examination booklet and the maternity check-up booklet.[11] New requirements for the "European Health Records" systems are also to be expected at the European level in the course of the implementation of the EHDS, which doctors will then also have to take into account in their documentation.

2.2. Data quality

In order to produce good data quality, which is necessary for successful data integration and analysis, the data must be allocated, marked and labelled (i.e., indexed[12]). For classification to be machine-readable, further steps of cleaning and curation are necessary. For example, measurement errors must be corrected or temporal gaps that can occur during medical handovers must be compensated for. In addition, the validity of each data set must be considered, i.e., whether the data credibly reflect what is claimed to be measured. Processes of data extraction, abstraction, generalisation and sample selection can introduce measurement error, noise, imprecision and bias ([17]: see p. 41).

Guidelines that define quality standards for data include requirements for data accuracy and precision, completeness, validity (representation of what is being measured), reliability, accessibility (openness, access rights), lineage (data lineage or origin, including mode of generation and processing) and provenance (who generated it). Such information should be provided by documenters in metadata to enable researchers to understand the suitability of the data for the intended analysis and to put the interpretation and use of the data in the right context [18].

So far, there are significant differences in the standards for data entry, collection and their coding, which is also related to the wide range of different clinical information systems and clinical documentation routines. This makes interoperability difficult.[13] Elaborate harmonisation and standardisation mechanisms are required if data from several clinics and practices or even EU-wide are to be merged across sites. This includes coordination mechanisms and negotiation processes between experts to assess data quality and informational content [19]. For research data that is to be processed by machine, experts also demand compliance with the FAIR principles (findable, accessible, interoperable and reusable).[14]

It must also be taken into account that physicians document and enter data differently, which influences the reliability and comparability of the data (uncontrolled interrater reliability). Bias in the secondary use of data from treatment contexts can also result from the fact that the course of a disease of seriously ill patients is documented in greater detail clinically and these data are thus disproportionately represented. Furthermore, biases in conclusions drawn from data analyses can occur if certain hospitals or wards specialise in particularly severe cases, which is reflected in large differences to data sets from other hospitals. Relating treatment outcomes directly to each other without taking these differences into account can lead to erroneous conclusions. In the case of billing data, there is also the danger of "upcoding", i.e., "generous" or unjustified diagnosing for business reasons. This impairs the validity of the data and the insights to be gained from them ([20]; [21]: see pp. 81–82).[15]

Another problem can result from the fact that, under the current design of the ePA, insured persons can choose which of their health data they want to release for research purposes. In the case of interdependencies between different diseases or treatments, considerable distortions can result if data is only selectively made available by the insured. Also, insofar as data from "wearables" or other non-professional data sources are included in health data sets, the reliability and validity of the data is hardly verifiable.

Overall, there are major challenges regarding the realistic representation, completeness and timeliness of the data in the establishment of the planned new data infrastructures from treatment

[11] For further information see https://www.kbv.de/html/mio.php (last accessed: 25.07.2022).

[12] To create an AI model, information must be fed to an algorithm so that it can process and deliver inputs and conclusions. This process can only occur if the algorithm recognizes and classifies the data fed to it. This process of assigning, marking or labelling data is called data annotation (see https://de.shaip.com/blog/the-a-to-z-of-data-annotation/ (last accessed: 22.09.2022).

[13] "The term interoperability refers to the function of information systems to exchange data and enable information sharing." (see https://edps.europa.eu/data-protection/our-work/subjects/interoperabilite_de, last accessed: 13.10.2022).

[14] See https://www.go-fair.org/fair-principles/ (last accessed: 15.11.2022).

[15] The 126th German Medical Congress 2022 also refers to this by pointing out the danger of data incongruence between electronically stored data and the actual state of health of patients, which can lead to unnecessary or even faulty treatments, in resolution Va – 10 "Faulty digital data as a health risk". In this context, the German Medical Congress calls for an internal debate within the medical profession on how this can be addressed in order to protect patients.

data that are to be integrated and used for research. Further challenges arise with regard to generalisability and proof of causality for research.

2.3. Data security

When data is to be merged and stored for long periods of time, another important aspect is ensuring data security. This requires secure servers, protection against data leaks and hacking. Both anonymisation or pseudonymisation and secure encryption of treatment data must be guaranteed in order to make unlawful re-identification of individual patients more difficult. But even with fully anonymised data, re-identification cannot be completely ruled out (cf. [22–24]). Data breaches, theft, blackmail through ransomware and unauthorised access are on the rise and have already been documented in German hospitals (cf. [21]: p. 84; [25–28]). A potential conflict can arise when balancing the protection of confidentiality or privacy with making data available for research.

With regard to the potential threat, a distinction can also be made as to whether data storage is centralised or decentralised. New analysis methods allow algorithms to be brought to the data (federated learning) and only the results to be retrieved, which is considered more privacy-friendly.

2.4. New approach to research

The aim of research with treatment data is to improve health care. This raises questions about the quality of research that operates with large amounts of clinical data: How can the chances of gaining foreseeable future knowledge be correctly assessed? Where are the risks, e.g., of over- or misinterpretation of the findings?

Essential characteristics of research with treatment data result from the sheer amount of data that is potentially available. In this context, the developments described above can also be placed in the ethical discourse on "Big Data" and the use of AI and ML in the research context [24, 29]. The new methods of information technology enable "data-driven" (or according to other authors: "inductive" [30]) approaches to research. This research with a high volume of treatment data is taking its place alongside previous research methods in medicine and differs greatly from the hypothesis-driven approach of previous medical research (such as the "gold standard" of randomised controlled pharmaceutical trials). Traditionally, this generates inductive exploratory hypotheses by means of individual clinical case observations, scientific laboratory findings, qualitative and quantitative social science and epidemiological approaches, and uses systematic research approaches for deductive testing of hypotheses and for establishing causal effects of drugs, medical devices or complex care models. What is new is that in "Big Data" research, the claim is sometimes made that this type of research is capable of both: the goal is to find inductively relevant questions in the data (usually supported or also primarily guided by ML and AI). Both in terms of scientific theory and in the derivation of practical consequences from study results, the question then arises as to the significance of those recognised correlations, for example, by means of ML. In 2008, Chris Anderson pointedly proclaimed the end of all theory in data-based research and the abandonment of systematic proof of causal relationships with the argument "Petabytes allow us to say: 'Correlation is enough'" [31].[16] In contrast, other authors point to the indispensability of systematic falsification of causality hypotheses – especially in the medical context, unlike in marketing contexts – for example in order to best estimate adverse drug reactions or to effectively address population-related risk factors in public health measures [34].

Ultimately, it remains of crucial importance not to unduly simplify the manifold reasons that can underlie a correlation of two variables. With regard to causal relationships, this means, for example, that the statistical correlation between variables A and B can be both an expression of a causal influence (effect of A on B or vice versa or complex interaction between A and B) and an expression of a common cause of A and B by C ([24]: see p. 68). Large and diverse amounts of data ultimately make it possible, above all, "to discover correlations between many more factors more quickly and better and also to develop new hypotheses about cause-effect relationships" ([24]: see p. 71), which can then be tested more closely by means of conventional, e.g., experimental, research.

Further quality issues stem from the fact that treatment data were not collected and compiled for the purpose of answering research questions, but are the more or less random result of various political, social, economic and technical factors. This may imply that those covariates that would be interesting to study from a scientific point of view have not been documented or have been insufficiently documented. Studies that operate with large pools of treatment data must face the challenge that it can be difficult to extrapolate the results of studies on large collectives to the ultimately smaller target population affected. As Caliebe et al. impressively demonstrate [35], the number of suitable "study participants" is often ultimately small, even with enormously large data sets, if specific research questions are used as a basis and inclusion and exclusion criteria are consistently applied. Since in the case of extremely large data sets the discovery of "any" correlations by ML occurs regularly, there is also the risk of an over- and false evaluation of the correlations discovered in this manner. Accordingly, the occurrence of "artefacts" (i.e., statements obtained through data analysis that have no counterpart in the real world) is virtually always present in large data sets. For this reason, methodological experts currently recommend using "Big Data" studies primarily to generate hypotheses, which are then tested in controlled studies in a second step [34]. In newer statistical research designs, possibilities are currently being developed and tested to link data from registries and randomised controlled study designs more closely and directly, for example by searching for test persons from registry data, comparing them and testing interventions systematically and also randomised [36, 37]. One of the advantages of research with treatment data is that databases with treatment data potentially contain information on outcomes that directly reflect clinical practice and are also of high clinical relevance (e.g., mortality or hospitalisation). In contrast, data that serve to deepen the understanding of biological processes (such as biomarkers) or social and psychological factors that influence health are generally not contained in treatment data in the same quality and to the same extent as in data sets that were collected within the framework of studies specifically designed for the relevant research question.

3. Ethical evaluation of current developments

High-quality patient care essentially depends on good medical research. Robust research findings must in fact be incorporated into

[16] Andersen's statement that "the numbers speak for themselves" if there is enough data, has been widely criticised and refuted; see [32, 33].

Deutsches Ärzteblatt | DOI: 10.3238/arztebl.zeko_sn_behandlungs daten2022_en

patient care. The use of treatment data from health care to gain scientific knowledge fundamentally promises to improve and accelerate medical research for the benefit of patient care. From an ethical perspective, however, the question arises under which ethical framework conditions the corresponding infrastructures can be established, promoted and maintained. Furthermore, it raises the question of how realistic the objectives are, to what extent practising physicians should participate and to what extent they should encourage patients to make their data available. For an ethical evaluation of the envisaged structures, this means that integrating them into the health care system and medical research in Germany must adequately take into account the professional ethics demands of physicians, the needs of patients and their families, and the values of our civil society. Both the rights and interests of those who make their data available and an "architecture of trust" (trust model) in the entire infrastructure of data processing and use are of vital importance here. In this respect, it is the duty of ethics to consider both the opportunities and the risks of procedures, structures and objectives in order to promote potential benefits and reduce potential harms. Particular attention must be paid here to the intended entanglement between the different spheres of data collection in the context of patient care on the one hand and its secondary use in the context of relevant research projects on the other. The ethical tensions between the logic of research and the logic of healing must be elaborated in such a way that they do not hinder each other to the detriment of patient welfare.

3.1. Ethical tensions between care and research contexts

Even if the use of treatment data for research has the common goal of improving patient care and gaining medical knowledge, their specific differences must be taken into account from an ethical and systematic perspective. This is because both are subject to different regulations and pursue different internal goals, which may well conflict. Patient care and research do not only meet different requirements institutionally and legally, but also ethically, according to the diversity of the rationale behind the goals of care (individual diagnosis, therapy, prevention, palliation) and research (supra-individual scientific generation of substantiated knowledge). The interconnection of these two spheres creates tensions (cf. [38]: see p. 15; [39]: see p. 68). Another special feature of medical research is the involvement of independent ethics committees to advise research projects. Such an obligatory external ethical-legal authority does not usually exist in connection with patient care. Bringing the two spheres of research and care together in a justifiable way through the use of treatment data in research is therefore an ethical challenge.

The point where the different rationales of medical research and care meet becomes problematic with regard to the secondary use of treatment data when care or the relationship of trust between patients and doctors suffers as a result. The well-being of patients must remain the primary goal of care. This could be undermined if the additional documentation effort is at the expense of the quality of care and the contact time with patients. The relationship of trust with physicians can also be disturbed if patients do not feel sufficiently informed about the benefits and risks of secondary use, if poor governance in data collection initiatives leads to data leaks, but also if physicians do not make patient data available for research to the extent that their patients expect [40].

In the case of research with treatment data, the research interest has a direct impact on the treatment context while also requiring the participation of physicians who have not been regularly involved in research projects. According to a recent survey, there are clear differences between research-oriented and purely clinical physicians with regard to the requirements they would like to see fulfilled in order to support the secondary use of treatment data [41]. While doctors at university hospitals are primarily concerned with data quality and privileged research use, doctors in private practice see data security and financial compensation for the additional personnel and time required as decisive prerequisites. From an ethical point of view, the distinction between the requirements of the treatment context and the secondary research use is therefore not only relevant with regard to the evaluation of the quality of the data and patient expectations. Rather, the distinction also plays a role with regard to the additional effort that physicians and other health professionals invest in data work as well as in education and information about data initiatives – this must not be at the expense of the primary treatment mandate. The potential risks with regard to the quality of patient care are manifold: On the one hand, it may simply be a question of the available working time of the health professionals, within which the serving of genuine (also psychosocial) patient interests may be put back in favour of "data work". There is also a fear that in the future the authentic concerns of the patient will be less in the foreground of the treatment discussion, but rather the demands that are placed on the practitioner by the software. In the worst case, it cannot be ruled out that the requirements of the "data work" will influence the diagnostic and therapeutic measures initiated, for example, by carrying out examinations solely (or predominantly) for the purpose of meeting the requirements of complete documentation demanded by the software.

When research and care are closely linked, there is also an increased risk of therapeutic misconception. This occurs when a person or the researchers themselves fail to recognise the difference between the needs of research and the treatment of care, and therefore wrongly or excessively attribute an individual therapeutic benefit to the research procedures ([42]: see V-57). Even if patients are asked by their treating physicians to make their data available for research, this can create false expectations of benefit. Slogans such as "heal with data" may raise expectations of a timely and individual benefit from the disclosure of treatment data. However, there is usually no direct benefit from research with treatment data for the "data discloser". Firstly, because the data have already been analysed in the treatment context and no additional or new data are collected, and secondly, because longer periods of time are needed for the generation of knowledge through research projects. Currently, it is only very rarely the case that a secondary use discovers surprising new correlations that were not yet recognised primarily and can be reported back to the treatment context in a timely manner.[17] Individual added value from new findings may sometimes arise in secondary research with treatment data, especially in imaging and genetic studies.[18]

[17] The proposal for a Regulation of the European Parliament and the Council of the European Union on the European Health Data Space (EHDS Regulation) provides for the following under Art. 38 (3): Should a national access point for health data be informed by a data user of a discovery that may have an impact on the health of a natural person, the access point for health data may inform the natural person and their treating health professionals of this discovery (this requires waiving anonymisation or pseudonymisation).

[18] It must be determined during project planning whether there is a possibility that additional findings will be generated within the framework of a project. Consent for secondary data analysis of primary clinical data must take this aspect into account.

3.2. Ethically relevant implications for the treatment context and society

Based on the ethical principle of autonomy, the debate on the release of personal data demands that informational self-determination always remains with the person from whom the data originates. Therefore, it must be precisely defined under which circumstances data of patients can be released, what role the attending physicians hereby have, what incentives there should be for this and how stigmatising or discriminatory consequences can be avoided by these processes as well as by the evaluation of the data. Doctors have a general obligation to provide support in accordance with § 346 para. 1 S. 1 SGB V (see section 4.4.) in the sense of appropriate information, which must not have a persuasive character. From a communitarian point of view, it should be noted that data literacy is not equally pronounced in all people, especially when it comes to digital data management. This then also affects the question of how a "broad consent" can be structured with regard to data use.

Special ethical and socio-political discussion and consideration is required if data provided from health care is not only to be used for therapeutic or diagnostic research, but also in the context of health economics and medical sociology, for example to compare the efficiency and quality of treatment in clinics or doctors' practices or to introduce new remuneration models. The same applies if the exchange of data is intended to take on the form of a trade with commercial character.

According to experiences from the highly digitalised Danish healthcare system, the real danger of healthcare workers engaging in "data massaging" is also indicated. This can include arbitrary, non-outcome oriented or even strategic data manipulation to meet the growing demands and requirements of digitised medicine or to pursue non-healthcare objectives [43]. This, in turn, may have the effect of eroding trust in the integrity and veracity of data. Moreover, "as data become a prime means of inter-organizational communication and a precondition for recognition, they can contribute to causing a shift in priorities of clinical attention away from patients and towards the signs involved in data exchanges" ([43]: see pp. 448 f.). In the long run, this could undermine professional and moral standards.

The opportunities of releasing treatment data must be weighed against the risks. The latter include restrictions or violations of privacy at the individual level. At the societal level, it must be considered that this can lead to a loss of trust in the health system, to a reduction of humans to data points, to suboptimal treatments, to medicalisation, to stigmatisation and to further downgrading in societal solidarity [44]. From the point of view of social justice, the discussion also calls for [45] the fact that without the availability of data, medical research could be inhibited and that both patients and doctors could demand participation in favour of the common good.

3.3. Patient autonomy

3.3.1. Informed consent and consent models

Patients have the right to informational self-determination, and this right is particularly important in the case of sensitive medical data. The patient's right to informational self-determination includes the right to determine whether and how personal data are processed (especially collection, storage, disclosure, use, see in detail section 4.1.1.), the right to object, correct and delete as well as to be informed about the use of medical data. In order to be able to exercise this right responsibly, patients must be informed about the opportunities and risks of data usage before they consent to or refuse it. Different models are being discussed for the time and scope of consent as well as the possibilities of control and adjustment by the patient.

In contrast to clinical studies with humans, for which the participants can and must be precisely informed about the goals, methods, expected benefits and risks before inclusion in the study, this is not possible for infrastructural projects. The aim of these is first to collect and process the data and only in a second step to make the data available for a specific research project. Here, risks and expected benefits can be generally indicated, but the concrete research question is still unknown and can only be narrowed down to the field of medical research. Consent for such a broad field of research is therefore called "broad consent".

In 2016, the World Medical Association adopted the Taipei Declaration on Research on Health Databases, Big Data and Biobanks, which complements the Declaration of Helsinki; it intends to restrict research with health data of collective benefit only as little as necessary, while still preserving the individual rights to autonomy, confidentiality and privacy for data sharers [46]. The Declaration therefore calls for obtaining consent for collection, storage and reuse. This may, however, cover a broad field if it is based on important information about the database and risk assessment on the one hand, and if a governance structure is established that is committed to transparency, data use and security on the other. Similarly, the "International Ethical Guidelines for Health-related Research involving Humans" of the Council for International Organizations of Medical Sciences (CIOMS) recognised broad consent or opt-out information as appropriate for those data collections where more specific information on the research question is not yet available at the time of data release [47].[19]

Practical considerations in particular are asserted in favour of broad consent, namely to facilitate medical research and to reduce the drop-out rate in the event of recontact within the framework of the informed consent model, as well as to satisfy the demand for data in Big Data and AI research [24, 50]. However, there is criticism that the purpose declaration of broad consent is very vague and that the term "health-related research", for example, as used in English-language documents, is hardly restrictable. This creates the danger of blanket consent, which undermines the principle of autonomy [48, 51].[20]

One model that combines data collection with control and information options according to patient preference is the so-called meta-consent [53]. Here, as part of consenting to the use of their treatment data for research, patients would indicate which types of data they would like to release immediately and how often and for which types of research projects they would like to be asked for permission separately instead. So far, the meta-consent has

[19] The MII meets certain transparency criteria as suggested above: Although it restricts the purpose for future research projects in broad consent exclusively to "medical research", it thus enables very different research projects without a more specific purpose statement at the time of consent. On the other hand, its website informs which research projects have been provided with data, thus facilitating a project-specific objection [48].
Regarding broad consent for future research purposes, see also "Chapter III – Obtaining and storage for future research" of the Council of Europe Recommendation CM/Rec (2016)6 of the Committee of Ministers to member States on research on biological materials of human origin [49].

[20] Blanket consent for processing personal health data for research purposes is considered inadmissible with reference to medical confidentiality as well as under data protection law ([52]: s. p. A 10).

Deutsches Ärzteblatt | DOI: 10.3238/arztebl.zeko_sn_behandlungs daten2022_en

been tested in one study: out of 1,000 invited subjects, 18 % could not use the meta-consent app due to lack of a suitable electronic device, and 40 % were already primarily not interested in participating in the study. The participation rate was therefore only 42 %. For the participants, the consent app offered the possibility to control the intensity of participation or the frequency of enquiries about study projects. Interestingly, depending on the type of data, between 50–75 % chose a broad consent setting as appropriate, i.e., they no longer wanted to be asked for permission separately for each use of data. The implementation of such a narrow feedback loop is thus conceptually better suited than broad consent to meet the differently pronounced control and information needs of patients. However, it poses its own data protection and information technology challenges and also limits the usability and, as the study above shows, the representativeness of the data.

3.3.2. Objection model (opt-out)

In contrast to the currently planned legal consent solution for ePA, the scientific expert opinion on "data donation" commissioned by the BMG proposes an opt-out solution [54]. It also deals with the consent-independent data processing option (opt-out model) and argues that the gained co-determination as to whether and which research one supports with one's data must be weighed against disadvantageous aspects such as the effort required for the information process and the poorer representativeness of the data of these models. The expert opinion of the German Council of Health Care Experts also highlights the need for a statutory regulation for the opt-out solution for the secondary use of ePA data [45]. This means that the health data of all citizens could be used as long as they do not individually object to the use. The opt-out model would have the advantage of a higher representativeness of the data sets and a better overall representation of the reality of health care. Initial surveys among patients (in this case in an oncological care context) indicate that patients are very willing to release their treatment data for research purposes [41, 55].

3.3.3. Pros and cons for the opt-in or opt-out solutions of data release for research

There are strong arguments in support of both an opt-in and an opt-out solution for research with treatment data. For both forms of implementation, further measures are necessary to ensure the integrity of the system.

The following arguments are put forward in favour of retaining a consent solution (opt-in) for the release of treatment data:

The consent of patients regarding the disclosure of their sensitive health data from the treatment context is in line with the ethical principle of autonomy and the right to informational self-determination of citizens in a liberal and democratic constitutional state. An objection solution, on the other hand, shifts the burden of proof from research to the patient. "Whoever remains silent consents" contradicts the practice in other medical and social contexts and is partly regarded as unconstitutional. Therefore, important aspects speak in favour of a consent solution. For this purpose, pragmatic models of broad consent and meta-consent are suitable (in addition to individual informed consent for specific research projects) in the context of building up a stock data infrastructure for research, accompanied by trust architectures such as trusts, ethics- and governance bodies, in order to guarantee the integrity of these data infrastructures. If patients were not asked for consent to share data, they could feel ignored and exploited. In addition, trust in the system could suffer [44, 48]. For example, broad consent is criticised not only for its vague purpose description, but also for the fact that it could open data access to purely commercially oriented companies without the knowledge of the persons concerned [53]. According to a recent survey, patients differentiate with regard to for whom and in what form they would release their health data: With regard to usage by private research institutions, the willingness to release data decreases considerably compared to usage by public health actors ([56]: from p. 42). Therefore, the maxim applies: the broader the consent is written, the stronger the corresponding trust architectures must be established. In order to support researchers in their justified request to be able to work with data from treatment practice, chambers and professional societies should help medical practices and hospitals to systematically inform patients about the importance of making individual health data available for medical research.

The following arguments are presented in favour of the introduction of an objection solution (opt-out) for the release of treatment data:

Both aspects of the practicability of research and the quality of research findings as well as empirical findings on patient preferences speak for an opt-out solution in the release of treatment data for research. Research based on large amounts of data ("Big Data") or data-driven research, which is to be realised with treatment data, can be all in all be sensibly implemented if these data sets from many areas are available as completely as possible. In the case of extensive information requirements for data release by patients, not only can potentially negative influences on the doctor-patient conversation be expected (dominance of research information over the topics in the treatment process that are of primary importance to the patients themselves), but it is also possible that ultimately only rather small and (at the population level) incomplete data sets will be transmitted. Sources of systematic biases in the data are manifold in an opt-in model: they can result from different care settings (possibly stronger motivation to participate in the inpatient sector or in specialist care) or also from socio-demographic characteristics. It is possible that the informative value of the data sets in the implementation of an opt-in model could ultimately be so low that research with treatment data on many questions (e.g., moderately common and rare diseases) cannot be meaningfully carried out.

The establishment of an opt-out solution must in any case be accompanied by a broad social debate and comprehensive information for the public. A broad-based information campaign would have to ensure that it is generally known that treatment data from the solidarity-funded health system will be used secondarily for research purposes unless an objection is raised. Such a clear and broadly communicated policy may ensure better informed consent than another consent form (broad consent), which has to be signed along with many others at the time of hospital admission or doctor's visit. There is a need for differentiation with regard to the question of whether all health data or only selected data should be used without consent and also with regard to the question of whether only data that will arise prospectively ("ex nunc") or data that already exist from the past ("ex tunc") will be used for research purposes ([57]: p. 4).

In order to ensure the right of revocation, it would be necessary to provide regular information about research purposes and institutions that have access to the treatment data, in order to enable patients to make a qualified choice to revoke through this transparency [48]. And finally, a corresponding national or EU-wide register or an explicit information would have to be provided in the ePA, which would keep the objection legally secure and confidential in a simple procedure ("easy-out").

Ultimately, lawmakers will have to make a decision on an opt-in or opt-out model (if necessary for different constellations) after intensive societal discussion. In doing so, international experiences should be critically evaluated.[21] Further empirical studies should clarify how critically citizens and patients view the various solutions and under which supporting measures they would possibly approve of a corresponding legal regulation.

3.4. Data governance and trust models

What the models of prior consent (e.g., broad consent) and the objection solution have in common is that they shift the responsibility for the control, risk-benefit assessment and accuracy of consent for future usage requests to third parties: to the research institution, ethics committees, data access committees, trustees or other supervisory structures of data governance, which are supposed to ensure the protection of patients' interests and research benefits. In regulatory terms, this means that the less control individual patients have over the use of their data, the higher the requirements must be for oversight bodies in terms of transparency, disclosure, accountability and credibility.[22] In this context, the EU's Data Governance Regulation also relies on the involvement of neutral data intermediaries. These can be, for example, independent trustees who manage patients' data in their best interests and according to their preferences in the sense of "stewardship", with fixed rights and obligations and only release patients' data to third parties according to certain defined criteria and procedures [62–64]. Data intermediaries or trustees must also fulfil transparency and accountability obligations towards data providers and the public. Ethics and governance bodies can also be established at such data trusts, which assume supervisory and co-decision rights and in which patient protection, data protection and consumer protection organisations are also represented. In addition, specialist scientific expert groups can be included with access committees as an additional quality check for the research projects. For the Big Data initiatives such as the MII[23] or data use via the ePA[24], appropriate oversight is under development and its structure can be reviewed. Currently, many so-called trustee or trust bodies at clinics do not meet the aforementioned requirements. This also applies to the so-called trust centre at the Robert Koch-Institute (RKI), which is responsible for the research data centre at the Federal Institute for Drugs and Medical Devices (BfArM), as this only carries out a two-stage pseudonymisation for the treatment data of patients with statutory health insurance, but does not fulfil any further supervisory, transparency and accountability obligations.

The importance of transparency and accountability for the integrity of organisations using or sharing care data for research is illustrated by the UK example of NHS care.data, a collaboration between the NHS Foundation and DeepMind Technologies, a wholly owned subsidiary of Google's Alphabet Inc. Concerns were centred on sharing pseudonymised medical information with commercial companies without the explicit consent of patients and the lack of communication about this. Finally, more than one million people objected to this use and the programme was terminated [65–68]. An unexpected effect was that patients withheld important information or stopped going to the doctor even though they needed treatment, for fear that the usage of the data would lead to stigmatisation, discrimination or other disadvantages for themselves (see [69–71]). In this context, it is reported from Denmark that coded psychiatric diagnoses such as ADHD or depression, which were made on patients in childhood in order to entitle them to school support and therapy, were to their disadvantage when they reached adulthood. These include long waiting periods for permission to get a driver's licence and the rejection of applications for admission to the military [60].[25]

It is clear from these data initiatives, as well as others for which trust has been withdrawn, that especially in the case of broad consent that is not project-specific, a number of other requirements must be met in order to ensure that the data is used in a socially accepted and trustworthy manner [76].

Beyond following legal norms, the concept of a "social licence" for data-intensive research postulates that researchers need to internalise certain principles and values such as orientation towards the common good, reciprocity and non-exploitation in order to act in a trustworthy manner. In addition, practical precautions are needed to ensure transparency, inclusivity and accountability [77]. These include regular quality assurance of the database itself, continuously updated technologies to ensure data security (including secure pseudonymisation and encryption), legitimacy checks of those authorised to access the database, assessment of study requests by an ethics committee and data release by an appropriate governing body. An example of this is the informed consent for data use, which was developed within the framework of the MII and allows health data to be used for medical research. This broad consent is compulsorily flanked with governance elements such as a model use policy and rules of procedure for data access committees, a handout for physicians on how to use the texts and several strategies on how

[21] The Danish case is particularly instructive: In Denmark, which is highly datafied, all citizens are assigned a ten-digit Central Personal Register (CPR) number. This number is used for almost all contacts with public authorities and also many private services. It allows data from health registers to be correlated with data from education, employment and income registers. Via Statistics Denmark, researchers can use this registered data for studies without consent and without the possibility of revocation by the data holders according to certain procedures designed to exclude re-identification. In 1995, an opt-out register (known as Researcher Protection) was established. Citizens could register with their CPR number if they did not want to be contacted for targeted studies. After more than 900,000 people, i.e. 16 % of the population, had registered their objection, the responsible ministry decided in 2014 that too many citizens who had registered there did not actually want to object to research. As a result, the opt-out register was abolished by parliament in 2014 without debate. This meant that, in turn, all Danish citizens became identifiable and approachable for research contact via the CPR. In turn, the opt-out register was deleted without notifying the registered citizens and without offering alternatives [58–60].

[22] See also the recommendations of the Data Protection Conference in the "Petersberg Declaration on Data Protection-Compliant Processing of Health Data in Scientific Research" from 24.11.2022, which, among other things, call for appropriate safeguards and measures as well as a statutory "research secret" (similar to an attorney-client privilege) [61].

[23] See https://www.medizininformatik-initiative.de/de/zusammenarbeit/arbeitsgruppe-data-sharing (last accessed: 21.10.2022).

[24] See https://www.gematik.de/datensicherheit (last accessed: 21.10.2022).

[25] A further scandalised example for broken trust is the Nightingale case: The US hospital management company Ascenion had stored patient data from 50 million patients of its 2,600 clinics in a Google cloud and granted this company access to diagnostic and treatment data, laboratory results and hospital reports, including names and dates of birth, without informing the treating physicians or patients [72, 73]. Another case from the USA is the Dinerstein versus Google lawsuit, in which the University of Chicago Medical Center and Google are accused of using data from ePAs of thousands of patients, who were considered de-identified, as training data for AI development, making them re-identifiable by means of time stamps and geolocation, and using the data to develop commercial products [74, 75].

Deutsches Ärzteblatt | DOI: 10.3238/arztebl.zeko_sn_behandlungs daten2022_en

to make data use transparent: These include tutorial videos, web-based information and explanations, and a website that lists the studies that have received data from the MII.

Another aspect of building trust is the effective sanctioning of data misuse and data leaks. This involves criminal sanctions such as fines. In Denmark, a collective model was established that, in the case of data protection violations and data misuse, not only penalised the researcher, but also his/her entire working group or institute from accessing data from the Danish Statistics Authority for a limited time period. This has apparently proven effective for compliance.[26] Another penalty mechanism is the exclusion from further funding measures.

The involvement of ethics committees complies with key ethical standards and promotes trust in data-intensive medical research. Sponsors or publication bodies also often request the advice of ethics committees. However, it is shown that the current ethical standards and supervisory structures do not yet adequately meet current developments; therefore, they call for further development of guidelines and regulatory instruments by the established ethics committees for non-traditional forms of data-intensive research (such as for research projects with AI) [73]. Ethics committees particularly require additional expertise from statisticians and data analysts for an appropriate assessment of research projects in the context of data-intensive technologies. At the national level, the need for harmonisation with regard to the heterogeneous practice across Germany in the ethical and data protection consultation of studies continues to be indicated, particularly by the medical collaborative research community. This is because the current ethical consultation process for multicentre research projects is characterised by "multiple structures" [78] and results in delays and additional financial burdens for such research projects [79, 80].

The fact that only the participating physicians are subject to legal regulation of the profession creates an asymmetry in research with health data. Against this background, experts are discussing and recommending that non-medical data processing companies should also be accompanied by specialised "data science" ethics committees [81, 82]. In addition, according to Marelli et al. [73], data governance boards with gatekeeping functions should be established to ensure ethical and normative conditions of health data use. They propose effective auditing and benefit-sharing mechanisms to ensure that health data collected in the public sector is not privately appropriated for proprietary technologies, but benefits the general public.

Legislators should establish data governance directed at data use, which tailors the scope and reach of data access to the ethical and societal desirability of different types of health research. This should ensure not only individual informational self-determination, but also the ethical and socio-political impact assessment of data-intensive Big Data and AI research projects in the health sector.

Finally, the German dual insurance system should not be disregarded under aspects of fairness: While the ePA is expected to be equally usable for those with statutory and private health insurance, the transmission of billing data according to §§ 303a ff. SGB V, which takes place by law and without consent, currently only affects those with statutory health insurance. In addition to the question of a fair distribution of risks (such as "data leaks"), this unequal treatment also potentially affects the quality of the research results generated from the data. The "selection bias" leads to a lack of representativeness, which – if not statistically corrected – can lead to misinterpretations and consequently faulty study results and guidelines.

3.5. Special responsibility and role of doctors

The treating physicians as well as the practices and clinics in which treatment data with a transfer option are generated do have a central function and responsibility for creating system trust if treatment data are to be transferred for research purposes. Several aspects that are essential for this are the responsibility of physicians. These include the clear primacy of the patient's well-being, above all in a direct concern that diagnostic and therapeutic primary care remains unaffected by additional work that the secondary research use of treatment data requires. Therefore, it must be clearly communicated to the patient that the secondary research use does not change the current treatment and that no disadvantages arise if consent is not given.

As a rule, patients have neither a direct advantage nor a direct disadvantage as a result of data usage. Nevertheless, a benefit for future patients is conceivable. Although a possible disadvantage for the patient providing the data due to data leaks or unauthorised re-identification of personal data is a small risk, it cannot be ruled out and patients must be informed about it. Consequently, it is also the responsibility of doctors to ensure proper disclosure and information about the risks and benefits of data initiatives.

Treatment data are sensitive in different ways. Special attention should be paid to potentially stigmatising data, for example from genetic or psychiatric diagnostics already conducted in adolescence, which can still be relevant in a later phase of the life of the person concerned and can have a detrimental effect in different contexts of societal participation. It is precisely here that doctors have a responsibility to provide appropriate information about the risks of sharing data in order to strengthen patient autonomy. Doctors should also be supported in this by anticipatory and concurrent risk assessments by scientific bodies.

Merely informing patients about confidentiality risks should not be the only way to address them; data initiatives have a duty to monitor and take appropriate measures to make the usage of data secure. By providing transparent information, doctors contribute to building trust in the system by relieving patients of the worry that they will no longer be able to disclose all important information in the doctor-patient conversation. However, providing good information is not resource-neutral. If time and personnel are not compensated for this, then the framework in which doctors provide support with information and education is limited by safeguarding the patient's well-being in primary care.

Many patients expect their doctors to provide data for research if they have given their consent [40]. Since the usability of the data depends, among other things, on the quality of the documentation and this, as described in section 2.1., is already time-consuming and personnel-intensive for quality assurance in primary care, additional data work is necessary. If the efforts necessary for secondary data use lead to additional expenditures – e.g., by documenting the metadata (see section 2.1.) or by entering data into different systems – then physicians must also consider when this is detrimental to the contact time and treatment of their patients. According to ethnographic studies from Denmark and Great Britain [12–14], the standardised collection

[26] Information from Professor Hoeyer in a hearing conducted.

and processing of electronic data is often perceived as "meaningless work" that takes time and resources away from the actual work on patients [43].

Data-intensive medicine is generally associated with the fear of a possible additional burden due to the increased documentation effort for physicians and other health professionals [40]. This is because if treatment documentation is to be used for research, this will probably influence the documentation routines in care itself ([21], see also section 2.1.), since the collection of larger amounts of data is necessary for later research use (or quality assurance) than for pure treatment documentation. In the medium term, the increased use of data from treatment contexts will also change job profiles and make new fields of work necessary for data integration and interoperability of data from different institutions [14, 83].

It becomes clear here how important it is to develop user-friendly software systems and technically interoperable solutions that make multiple documentation obsolete (e.g., through more digitised primary documentation that could be simultaneously used for secondary data use) on the one hand, and how important it is to factor in and compensate for documentation efforts on the other. This is a huge challenge, especially in view of the shortage of skilled workers.

4. Legal aspects

Physicians are subject to a multitude of regulations both when collecting and transmitting patient data to third parties for their research and when using such data for their own research, which makes the legal situation incoherent and requires improvement.

4.1. Data protection legislation

The most relevant regulations are the General Data Protection Regulation (GDPR), the Federal Data Protection Act (FDPA) and the Federal State Data Protection Acts (LDSG). Medical specialist laws partly provide for sector-specific data protection provisions. Data protection law applies to the "processing" of personal data; this includes both the collection and use of patient data by doctors for their own research and the disclosure of patient data to third parties for their research (cf. Art. 4 (2) GDPR). Data that are (effectively) anonymised are not legally considered personal data and are therefore not subjected to data protection law.[27] Data are considered anonymised if they cannot (or can no longer) be assigned to a specific person. The extent to which the reference to a person is actually excluded is, however, legally disputed due to the existing and further increasing technical possibilities of re-identification.[28] Anonymisation must be distinguished from pseudonymisation, i.e., the processing of personal data in such a way that it can no longer be attributed to a specific data subject without the use of additional information, provided that this additional information is kept separately and is subject to technical and organisational protection measures (Art. 4 (5) GDPR). Pseudonymised data are still considered personal data and are subject to data protection law (see recital 28 of the GDPR).[29]

The same requirements apply to the transfer of personal data to project partners based in another EU or EEA state as to a transfer within Germany.[30] Personal data may be transferred to third countries or international organisations if the EU Commission has decided that an adequate level of protection exists there (Art. 45 GDPR). In the absence of such an adequacy decision (e.g., with respect to the USA[31]), the transferring authority must provide "appropriate safeguards" for data protection (see Art. 46 (2), (3) GDPR) and the data subjects must have enforceable rights and effective remedies. If such "appropriate safeguards" are also lacking, the data transfer is only permissible if an exceptional circumstance pursuant to Art. 49 (1) GDPR exists; this includes, in particular, the explicit informed consent of the data subject. The procurement of data from third countries is initially governed by the regulations applicable there; insofar as there is a personal reference, the requirements of the GDPR also apply to the processing of these data.[32]

In accordance with the GDPR, the processing of particularly sensitive personal data such as health data is only permissible on the basis of the consent of the data subject (see section 4.1.1.) or on the basis of a statutory authorisation (see section 4.1.2.). In addition, the processing agency is subject to a number of procedural requirements.[33]

The rights of patients to information on data processing, correction of incorrect data, deletion of collected data, restriction of data processing and objection to data processing (see Art. 15–21 GDPR) are exceptionally restricted if these rights are likely to make it impossible or seriously impair the realisation of the research or statistical purposes and the restriction is necessary for the fulfilment of the research or statistical purposes (Art. 27 para. 2 p. 1 FDPA).[34]

4.1.1. Processing treatment data for research purposes with patient consent

Health data are personal data relating to the physical or mental health of a person (including the provision of health services) and which reveal information about that person's state of health (Art. 4 (15) GDPR). The term is to be understood broadly and, in addition to purely medical data, also includes, for example, data collected by health apps or wearables such as smartwatches (e.g., pulse, blood pressure, body fat percentage); by contrast, it does not include data that relate solely to lifestyle and only indirectly allow (statistical) conclusions to be drawn about the state of health (e.g., the fact that a person is a smoker) [88].

The processing of health data is permissible, among other things, if the explicitly informed (Art. 4 (11), Art. 7 (4) GDPR) data subject expressly and voluntarily consents to the processing of their data for one or more specified purposes (Art. 9 (2) (a) GDPR – opt-in).[35] The data controller (see Art. 4 (7) GDPR)

[27] [84]: s. p. 603 (605, 625) with further ref.
[28] Details [85]: s. p. 143 ff.; [86]: s. p. 12 ff.; s. also [24]: p. 138 ff.
[29] Details [84]: s. p. 603 (605 ff.).
[30] [87]: s. p. 174.
[31] CJEU, Ruling from 06.10.2015 – C-362/14; CJEU, Ruling from 16.07.2020 – C-311/18.
[32] [87]: s. p. 181 ff.
[33] Pursuant to Art., 30 GDPR, the processing authority must keep a written or electronic register of all processing activities that are subject to its responsibility. According to Art. 30 I 2 GDPR, the directory must contain, among other things: the contact details of the controller (see Art. 4 (7) GDPR); the purposes for which the processing is carried out; a description of the categories of data subjects and data; the categories of recipients to whom the personal data are disclosed; where applicable, transfers to third countries or international organisations; if possible, the time limits envisaged for the deletion of the various categories of data; and, if possible, a general description of the technical and organisational data protection measures taken pursuant to Art. 32 I GDPR. If sensitive data such as health data (see Art. 9 I GDPR) are processed extensively in the context of a medical research project, a data protection impact assessment must be carried out in advance (for the content requirements see Art. 35 VII GDPR; [87]: see p. 134 ff.).
[34] The right to information pursuant to Art. 15 of the GDPR also does not exist if the data is required for the purposes of scientific research and the provision of information would require disproportionate effort (§ 27 para. 2 sentence 2 FDPA).
[35] The requirements for consent to the processing of certain treatment data for research purposes are in some cases further specified in national law, see for example § 11 III GenDG.

Deutsches Ärzteblatt | DOI: 10.3238/arztebl.zeko_sn_behandlungs daten2022_en

must be able to prove consent (Art. 7 (1) GDPR), which is why consent should be given in written form. Consent can be revoked at any time, whereby revocation of consent does not affect the lawfulness of the processing carried out on the basis of consent until revocation (Art. 7 (3) p. 1 and 2 GDPR). The data subject must be informed of the possibility of revocation prior to his or her consent (Art. 7 (3) s. 3 GDPR). If pre-formulated consent forms are used in a large number of cases, the AGB law of §§ 305 ff. BGB apply; in particular, such forms may not contain any unexpected or ambiguous clauses and the provisions must be clear and understandable [89].

The purposes to which the consent refers must be sufficiently specific (Art. 4 (11) GDPR). In the case of research-related processing of treatment data, the requirements for the specificity of consent, i.e., how specifically the content, purpose and extent of the data processing are to be defined, have not been bindingly determined. In particular, it has not been conclusively established to what extent "broad consent" to data processing for a "broad field of research" meets the requirements of the GDPR.[36 37] This is relevant for the use of treatment data for medical-scientific research purposes because, in contrast to clinical studies with humans, the specific research project or the specific research question is often still unknown at the time of consent, so that consent can only be obtained in general for purposes of medical research or medical research areas (e.g., cancer research).

The federal legislator allows consent for the processing of personal data in social security law both "for a specific research project" and "for specific areas of scientific research" such as "medical research"[38] (§ 67b para. 3 p. 1 SGB X; in reference to the ePA, also § 363 para. 8 SGB V).[39] The sample text for patient consent of the MII [40] also provides for broad consent to processing patient data "for medical research", which the Data Protection Conference of the Independent Data Protection Authorities of the Federation and the Federal States (DSK) has declared to be legally permissible.[41] This is in line with recital 33 GDPR, which states that it "is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection", which is why "data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research." In the context relevant here, these recognised ethical standards particularly include the Declarations of Helsinki and Taipei as well as the requirements of the codes of the medical profession (see section 4.3.).[42] Ultimately, the permissibility of broad consent also follows from the right to informational self-determination (Art. 8 CFR), which, in addition to the right not to disclose, also includes the right to disclose personal data.[43]

The parallel to the permissibility of further processing of personal data collected on a legal basis for purposes that are specified, explicit and legitimate "for scientific research purposes" (Art. 9 (2)(j) in conjunction with Art. 5 (1)(b) and Art. 89 (1) GDPR) supports the permissibility of broad consent also in the case of consent-dependent data processing for research purposes.

In the opinion of the Data Protection Conference (DSK), in cases where broad consent appears to be absolutely necessary to achieve the purpose of the research, more specific safeguards and guarantees for transparency, trust-building and data security are to be taken.[44] The measures must be documented and submitted together with the research concept, to the authorities responsible for approving the ethical and data protection compliance of the research project.

There is currently a high degree of legal uncertainty, which would be remedied by a statutory regulation of broad consent.

The requirements for consent concerning the processing of treatment data for research purposes have been partially specified or supplemented in national legislation. For example, when processing particularly sensitive personal data, such as the health data of patients, the consent must explicitly refer to this data according to § 51 para. 5 FDPA. According to the Genetic Diagnostics Act, the results of genetic examinations or analyses that were (also) carried out for medical purposes and not solely for research purposes (s. § 2 para. 2 (1) GenDG) may only be disclosed by the responsible medical personnel to persons other than the data subject with the express written or electronic consent of the data subject (§ 11 para. 3 GenDG).

Due to the current "patchwork" of existing legal permissions for the use of treatment data for research purposes and the associated legal uncertainty (see section 4.1.2.), medical practice should primarily make use of declarations of consent under the current legal situation [84].

4.1.2. Legal permission to process treatment data for research purposes

Processing personal health data for scientific research purposes without consent is permissible if a sufficient statutory basis for this exists (Art. 9 (2)(j) GDPR).[45] In addition, the general principles for processing personal data must be upheld. This includes, firstly, that the data is only collected for specified, clear and legitimate purposes and is not further processed in a manner incompatible with these purposes (principle of purpose limitation, Art. 5 para. 1 lit. b half-sentence 1 GDPR).[46] In the case of further processing for scientific research purposes, however, the principle of purpose limitation is considered to be observed (Art. 5 para. 1 lit. b. in conjunction with Art. 89 para. 1 GDPR, so-called secondary data use).[47] Secondly, processing personal data must be limited to what is necessary for the processing purposes (data minimisation, Art. 5 (1) (c) GDPR).[48] Accordingly, health data to be processed for

[36] See, for example [90–93]. Justifiably in favor of the permissibility of broad consent: [94] with further comments in favor of this view. Different view: Fröhlich/Spiecker [95], who, however, overlook the fact that the exception to the principle of purpose limitation in the case of further processing of data for research purposes under Art. 5 para. 1 lit. b GDPR also controls the consent requirement within the meaning of Art. 4 (11) GDPR. In the case of further processing of health data for scientific research purposes, consent need not relate to a specific case because of Art. 5 para. 1 lit. b GDPR. Moreover, Fröhlich/Spiecker disregard recital 33 to the GDPR, which explicitly legitimises broad consent.

[37] Other forms of consent under discussion, such as meta-consent (see 3.3. in the ethics section), as proposed e.g. by the Data Ethics Commission [64], are unclear in terms of their specific form and legal feasibility.

[38] [96]: s. p. 147; s. also [54]: p. 96.

[40] Accessible at: https://www.datenschutzkonferenz-online.de/media/pm/MII_AG-Consent_Einheitlicher-Mustertext_Einwilligung_v1.6d.pdf.

[41] Resolution of the DSK from 15.04.2020, accessible at: https://www.datenschutzkonferenz-online.de/media/dskb/20200427_Beschluss_MII.pdf.

[42] [85]: s. p. 112.

[43] Most recently Federal Constitutional Court (BVerfG) 152 (188, Rn. 84) with further ref. from the established case law of the BVerfG; from the scholarly writings instead of many [94, 98, 99].

[44] See resolution of the DSK from 03.04.2019, accessible at: https://www.datenschutzkonferenz-online.de/media/dskb/20190405_auslegung_bestimmte_bereiche_wiss_forschung.pdf.

[45] Details [100].

[46] S. also [24]: p. 131 f.

[47] Details [101].

[48] Cf. [24]: s. p. 132.

research purposes shall be pseudonymised insofar as this does not thwart or significantly impede the research purpose.

German legislature has made use of the possibility to allow the processing of personal health data for research purposes without consent in a large number of laws. This has resulted in a patchwork of different and partly fragmentary regulations scattered across federal and state levels. This leads to legal uncertainty and does not meet the new needs of medical research.

According to the FDPA, which applies to all general practitioners and specialists in private practice, doctors in state and private hospitals, and doctors in medical care centres (MVZ), the state hospital laws or state data protection laws apply to hospital doctors and doctors in state institutions, unless processing personal health data without the consent of the patient is permissible for scientific research purposes if the processing is necessary for these purposes and the interests in the processing significantly outweigh the interests of the person concerned (§ 27 para. 1 s. 1 FDPA). The health data must always be anonymised as soon as this is possible according to the research purpose (§ 27 para. 3 s. 1 FDPA). Until anonymisation, the health data and the data suitable for identification must be stored separately, unless the research purpose requires their combination (§ 27 para. 3 s. 2 FDPA). The publication of personal data is only permissible with the consent of the persons concerned (§ 27 para. 4 FDPA).

When using social data (see § 67 para. 2 SGB X) of the social service providers for research purposes, the provisions of §§ 75 f. SGB X must be observed. Doctors who do not work for a public body must undertake to process the data only for the intended purpose before transmitting and processing the social data to them (§ 75 para. 4 s. 3 SGB X). They are subject to supervision by the competent State Data Protection Authority (§ 75 (6) SGB X).

For processing patient data for research purposes by hospital physicians, the hospital laws of the states provide for special regulations.[49] The transfer of patient data to third parties for research purposes usually requires either the explicit consent of the persons concerned or an overriding public interest in the research project. The use of already stored patient data for own research is partly subject to less strict requirements.

To the extent that the cancer registries maintained by the Federal States (see § 65c SGB V) serve scientific research (see § 65c para. 1 (10) SGB V), the requirements for the transmission of patient data to the cancer registry and for the inspection of the data stored there are governed by State law.

Personal data generated in connection with organ transplantation may be processed for research purposes under the conditions of § 14 para. 2a of the Transplantation Law (TPG).

4.2.Medical confidentiality

In their capacity as doctors, doctors are not allowed to disclose information about their patients and in particular their secrets to third parties without authorisation according to the model professional regulations of the Federal Data Protection Act and Criminal Code (§ 9 MBO-Ä, § 1 para. 2 s. 3 FDPA, § 203 StGB).

If patient data is effectively pseudonymised or anonymised, the disclosure of this data to third parties does not constitute disclosure.[50] Such anonymisation or pseudonymisation is, however, not possible for all data sets.[51]

In such cases, the decisive factor is whether disclosure to third parties is permitted by the consent of the person concerned or provided for by law. A right or obligation to disclose may result from a (data protection) legal obligation to transfer patient data, as provided for in part by the State Cancer Registry Acts and the State Hospital Acts.[52]

4.3. Professional obligations of physicians conducting research

Physicians who participate in research projects in which the psychological or physical integrity of a human being is interfered with or in which bodily materials or data that can be attributed to a specific human being are used, must observe the Declaration of Helsinki of the World Medical Association (DoH) and, as a matter of principle, ensure that before the project is carried out, a consultation is held which is aimed at the professional ethical and legal questions involved and which is carried out by a competent ethics committee (§ 15 MBO-Ä).[53] According to section 32 of the DoH, doctors must obtain informed consent for the collection, storage or reuse of such research. If obtaining consent is on exception impossible or impractical, the research project may only be carried out after the assessment and approval by an ethics committee. The extent to which these requirements also apply to pseudonymised data has not yet been legally determined.[54]

The establishment and use of health databases (and biobanks) by doctors for research purposes is the subject of the Declaration of Taipei[55] of the World Medical Association. Among other things, special requirements apply to the education of data providers as a prerequisite for valid informed consent (No. 12). For the establishment of health databases, the approval of an independent ethics committee is also required (No. 19). Furthermore, special governance structures, such as regulations on the duration of storage, on the deletion and destruction of data, on the verifiable documentation of processing procedures, on the protection of the dignity, autonomy and privacy of the persons concerned, on the prevention of discrimination and on the authorisation of usage, as well as technical measures to prevent unauthorised access, should be established and persons responsible for this should be appointed (see No. 21).

4.4. Support obligations of contracted physicians and physicians in authorised hospitals for processing data in the ePA

Persons with statutory health insurance can voluntarily release data from their ePA for certain research purposes (§ 363 para. 1 SGB V). The transmission of the released data takes place to the research data centre (§ 303d SGB V) and requires the informed consent of the insured person (§ 363 para. 2 p. 1 SGB V). Insured persons can freely choose the scope of data release and limit it to certain categories or to groups of documents and data sets or to specific documents and data sets (§ 363 para. 2 p. 3 SGB V). The

[49] E.g. § 17 KHG LSA, § 39 BremKrhG, § 27 Abs. 4 BayKrG, § 34 SächsKHG, § 14 SKHG, § 25 BlnLKG, § 6 GDSG NRW. Subsidiarily, the respective State Data Protection Act (LDSG) applies (for public clinics) or the Federal Data Protection Act (FDPA) (for private clinics). A presentation of the relevant regulations in all Federal States can be found in [86]: s. p. 123 ff.

[50] [102] w. f. r.

[51] [54]: s. p. 92 f.

[52] [85]: s. p. 233; [54]: s. p. 115; details [103].

[53] Details and deviations may result from the professional regulations of the state medical associations.

[54] On the problem [54]: s. p. 116 f.; [86]: s. p. 298 ff.

[55] Accessible at: https://www.wma.net/policies-post/wma-declaration-of-taipei-on-ethical-considerations-regarding-health-databases-and-biobanks/.

release is documented in the ePA (§ 363 para. 2 s. 4 SGB V). The research data centre may make the released data available to various authorised users such as university hospitals (§ 363 para. 4 SGB V). Alternatively, insured persons may also make the data of their ePA directly available for a specific research project or for specific areas of scientific research on the basis of informed consent (§ 363 para. 8 SGB V).

Contract physicians and physicians in authorised hospitals have an important support function in the use of the ePA by insured persons.[56] On request by the patient, they must provide support in processing their medical data (§ 341 para. 2 SGB V) from the specific current treatment in the ePA (§ 346 para. 1 s. 1 SGB V).[57] This includes, in particular, assisting patients with the initial data entry into the ePA (§ 346 para. 3 s. 1 SGB V), the transmission of medical data into the ePA (§ 346 para. 1 s. 2, para. 3 s. 2 SGB V) and its storage (§ 347 para. 2, § 348 para. 2 SGB V). Physicians can transfer support tasks to professional assistants "insofar as these are transferable" (§ 346 para. 1 s. 4, para. 3 s. 3 SGB V). These are likely to be tasks that are not exclusively the responsibility of physicians or legally assigned to them.

Doctors must inform their patients that they can request that treatment data be transferred to the ePA and stored there (§ 347 para. 2, § 348 para. 2 SGB V). Information and education about the function and use of the ePA, on the other hand, has so far been the responsibility of the health insurance companies.[58]

4.5. Developments at the EU level

The European Data Governance Act published on 30st May 2022, which will be effective from 24th September 2023 [105], aims to promote the availability of data for research purposes and particularly to facilitate the voluntary provision of data by individuals and companies to recognised organisations for the benefit of the general public, such as namely medical research purposes ("data altruism"). A common European consent form for data altruism will be developed to facilitate the collection of data for data altruism purposes.[59]

The proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space (EHDS) [106], submitted on 3rd May 2022, aims, among other things, to obligate data holders (primarily organisations and institutions in the health and care sector) to transfer certain data to access points to be established by the Member States for the purposes of scientific research in the health or care sector. The European Commission has defined categories of data to be transferred (Art. 33, 41 EHDS draft Regulation). In addition, each data holder is to provide the access point with a general description of the data set they hold. If non-personal electronic health data are stored, they should be made accessible with the help of trusted open databases. If data holders violate the transmission obligations, the access points shall be able to impose fines and, in the case of repeated violations, exclude the data holders from participation in the EHDS for a period of up to five years (Art. 43 para. 5 EHDS Regulation). Once the Regulation enters into force, it is binding in its entirety and directly applicable in the Member States. The Member States may retain regulatory leeway within the framework of opening clauses. In addition, they may adopt legal acts for the implementation of the Regulation.

5. Summary and recommendations

In the course of increasing digitalisation of the health care system, demands for making treatment data from outpatient and inpatient care available for research purposes are growing. Physicians are faced with the challenge of educating patients about the usage of research, documenting their treatment according to appropriate digital formats and expanding their understanding of data-intensive research. Nevertheless, the treatment data are usually not simply available, but must be collected in a structured and standardised form, which entails considerable additional documentation work. From ZEKO's point of view, the considerable additional documentation work currently mainly required from service providers, requires special attention so that no negative effects on the relationship between doctors and patients result. In order to bring together data from clinics and practices, and in the future even across locations throughout the EU, harmonisation and standardisation mechanisms to ensure interoperability and data quality, as well as to avoid multiple documentation, are also necessary to a large extent.

High-quality patient care depends to a large extent on good medical research and on the fact that robust research results are actually incorporated into patient care. From ZEKO's point of view, the use of treatment data from health care to gain scientific knowledge in principle promises an improvement and acceleration of medical research for the benefit of patient care. The extent to which the use of treatment data for research actually achieves the intended goals of improving health care and outweighs the risks and resulting burdens, requires continuous evaluation and consideration.

In its ethical evaluation of the current developments, ZEKO primarily addresses the establishment, promotion and maintenance of the ethical framework of the new data infrastructures and corresponding governance and trust models, but also how realistic the objectives of the new research approaches are, the implications for patient autonomy and the extent to which patients and practising physicians should participate in it.

Physicians will play a central role in creating acceptance and trust in the system of the new type of research. In order to support and guarantee this, ZEKO believes that the following recommendations in particular should be taken into consideration:

Documentation and data work

- Uniform documentation standards are crucial for data quality and therefore require corresponding competence of the participating physicians (support for methodological competence, networking standards, interoperability guidelines, etc.).
- The various efforts should be promoted not only to electronically record the primary treatment documentation, but also to create an interface to enable secondary data use. For this purpose, user-friendly software and interoperable solutions should be developed in order to reduce the additional documentation effort, at least in the long term.
- If documentation obligations for research are expanded, a new, special professional group of data documentarians should be created in the medium term to perform such tasks in

[56] Since 01.01.2021, doctors have received a one-off payment of 10 euros for support services during a period of twelve months for each initial data entry (§ 346 para. 5 SGB V).
[57] Outside of the current treatment, physicians have no support obligations for the use of the ePA by insured persons. In particular, they are not obligated to transfer medical data collected prior to the current treatment to the patient file; [104]: s. p. 174.
[58] German Parliament printed matter 19/20708, p. 174.
[59] S. recital 52 and Art. 25 of the Regulation (EU) No. 2022/868 [105].

order to relieve doctors and other health professionals from additional data work.
- The documentation effort for the provision of treatment data for research purposes must be adequately remunerated. However, an appropriate compensation for doctors and other health professionals must not be so high that it constitutes an undue incentive to persuade patients to disclose data.

Education of patients and assurance of patient well-being
- Doctors are encouraged to proactively approach patients with regard to making their treatment data available for research purposes.
- Concerning the education of the patient, it is important to convey that the main focus is on primary care unhindered by any secondary use of treatment data.
- Informing the insured person about the ePA is a demanding task that can only partly be taken over by doctors. In the future, more complex questions about the ePA may require the establishment of counselling centres that can provide citizens with independent advice on their data management.
- There is a need to develop guidelines according to high standards for the release of treatment data for research on the part of the medical profession and government actors in the sense of neutral information, which support the proper information and education of patients by doctors.
- Patient expectations regarding confidentiality in the relationship with doctors must be fulfilled so that patients do not conceal or misrepresent disease-relevant information for fear of misuse.
- The additional educational and documentation effort for the research-based use of treatment data must not be at the expense of primary care. If the quality of primary care is at risk, doctors must prioritise the patient's well-being and the primary treatment mandate.

Ensuring trust in the systems and their integrity
- Efforts should be made to eliminate the existing patchwork of legal regulations that allow the processing of treatment data for research purposes without the consent of the persons concerned. The situation is not in compliance with the requirements of medical research and creates legal uncertainty. As long as legal inconsistency persists, medical practice should primarily rely on declarations of consent to legitimise data processing.
- Control over the data, in the context of informational self-determination, should remain with the patient (in accordance with the consent obtained), providing there is no statutory fact to the contrary.
- If broad consent is obtained, the principle must be that the broader the consent obtained, the stronger the robust compensation mechanisms for integrity and trustworthiness must be (governance and trust architectures including independent trustees, ethics committees, access and use committees, usage regulations and other technical precautions).
- With regard to the release of treatment data for research purposes with the consent of the patient (opt-in), the legislator should explicitly regulate the possibility of broad consent and define the necessary protection and security measures within the framework of a trust and governance architecture in order to eliminate the existing legal uncertainty.
- There are strong arguments in favour of both an opt-in and an opt-out solution for research with treatment data, which serve to strike a balance between the right to self-determination of the patient and the needs of research. For both forms of implementation, further measures are necessary to ensure the trustworthiness of the system. Depending on the different sensitivity of data constellations, different regulatory models (opt-in/opt-out) should be considered for the provision and usage of treatment data.
- If the legislator creates a cross-sectoral regulation that allows all treatment data to be processed for scientific research purposes if patients do not object (opt-out), it must be regulated in this case for which research purposes pseudonymised data are necessary and in which cases anonymised data are sufficient. In the case of legal permission to further process patient data for research purposes, it is mandatory for the data subjects to have an opt-out right according to the GDPR (Art. 21 (6) GDPR).
- Appropriate transparency, monitoring and accountability structures must be created to ensure data security, compliance with ethical standards and the protection of fundamental patient rights in data handling, processing and access. Therefore, the establishment of trustee bodies as intermediate, independent authorities, as required by the Data Governance Act and the EHDS, should be welcomed and promoted. Advocates of patient protection, data protection and consumer protection interests should be represented in data governance bodies.
- From ZEKO's point of view, the participation of advisory ethics committees (in future also for data processing institutions or researchers who are not themselves medical doctors) is essential, as it meets central ethical standards and promotes trust in data-intensive medical research. However, the ethical supervision of "Big Data" studies requires new expertise with regard to the methodological, ethical and legal particularities of data-intensive technologies and research. Patient protection organisations should also be represented when forming the ethical review boards.
- The unauthorised use of data and its abuse must be adequately sanctioned. Regulatory protection mechanisms (criminal/legal and technical) to compensate for the risks associated with secondary use are urgently needed (e.g., punitive sanctions for misuse of data, temporary exclusion from data access, exclusion from further funding measures, deletion procedures and further measures to protect against discrimination through classification in certain groups).

Literature

1. Bundesministerium für Bildung und Forschung (BMBF): Daten helfen heilen. https://www.bmbf.de/bmbf/shareddocs/kurzmeldungen/de/daten-helfen-heilen.html (last accessed on 9 September 2022).
2. Bundesministerium für Bildung und Forschung (BMBF): Medizininformatik: Ein Schatz, den es zu heben gilt. https://www.bmbf.de/SharedDocs/Videos/de/bmbf/7/73/7395_medizininformatik-ein-schatz-den-es-zu-heben-gilt.html (last accessed on 9 September 2022).
3. Caliebe A, Antes G, Leverkus F, Krawczak M: Dateninfrastruktur: Ein Baustein gegen COVID-19. Dtsch Arztebl 2021; 118(10): A-501 / B-423.
4. Heaven WD: Hundreds of AI tools have been built to catch covid. None of them helped. https://www.technologyreview.com/2021/07/30/1030329/machine-learning-ai-failed-covid-hospital-diagnosis-pandemic/ (last accessed on 21 September 2022).
5. Europäische Kommission: Verordnung über Daten-Governance – Fragen und Antworten. https://ec.europa.eu/commission/presscorner/detail/de/QANDA_20_2103

Deutsches Ärzteblatt | DOI: 10.3238/arztebl.zeko_sn_behandlungs daten2022_en

(last accessed on 22 September 2022).

6. Europäische Kommission: Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über europäische Daten-Governance (Daten-Governance-Gesetz). https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52020PC0767&from=DE (last accessed on 21 September 2022).
7. Gitelman L: „Raw data" is an oxymoron. Cambridge, Massachusetts: The MIT Press 2013.
8. Petersen AR: Digital health and technological promise: A sociological inquiry. London: Routledge 2019.
9. Miotto R, Wang F, Wang S, Jiang X, Dudley JT: Deep learning for healthcare: review, opportunities and challenges. Brief Bioinform 2018; 19(6): 1236–46.
10. Sheikhalishahi S, Miotto R, Dudley JT, Lavelli A, Rinaldi F, Osmani V: Natural Language Processing of Clinical Notes on Chronic Diseases: Systematic Review. JMIR Med Inform 2019; 7(2): e12239.
11. Lusignan S de, Weel C van: The use of routinely collected computer data for research in primary care: opportunities and challenges. Fam Pract 2006; 23(2): 253–63.
12. Swinglehurst D, Greenhalgh T: Caring for the patient, caring for the record: an ethnographic study of ‚back office' work in upholding quality of care in general practice. BMC Health Serv Res 2015; 15: 177.
13. McVey L, Alvarado N, Greenhalgh J, et al.: Hidden labour: the skilful work of clinical audit data collection and its implications for secondary use of data via integrated health IT. BMC Health Serv Res 2021; 21(1): 702.
14. Bossen C, Pine KH, Cabitza F, Ellingsen G, Piras EM: Data work in healthcare: An Introduction. Health Informatics J 2019; 25(3): 465–74.
15. Beckmann M, Sell C, Aydogdu M, et al.: Dokumentationsaufwand und verbundene Ressourcen bei Patientinnen mit einem primären Mammakarzinom – von der Primärdiagnose bis zur Abschluss der Nachsorge – Ergebnisse der multizentrischen Erhebung. Gesundheitswesen 2016; 78(7): 438–45.
16. Cornelius F: Krebsregister: Bewertung der aktuellen Situation. Uro-News 2021; 25(11): 34–9.
17. Kitchin R: Data lives: How data are made and shape our world: Bristol University Press 2021.
18. Batini C, Cappiello C, Francalanci C, Maurino A: Methodologies for data quality assessment and improvement. ACM Comput Surv 2009; 41(3): 1–52.
19. Petersen I, Kollek R: Digital Scientific Practice in Systems Medicine. In: Lessenich S (ed.): Routinen der Krise – Krise der Routinen. Verhandlungen des 37. Kongresses der Deutschen Gesellschaft für Soziologie in Trier 2014; 1783–1792.
20. Jungkunz M, Köngeter A, Mehlis K, Winkler EC, Schickhardt C: Secondary Use of Clinical Data in Data-Gathering, Non-Interventional Research or Learning Activities: Definition, Types, and a Framework for Risk Assessment. Journal of Medical Internet Research 2021; 23(6): e26631.
21. Jungkunz M, Köngeter A, Winkler EC, Mehlis K, Schickhardt C: Sekundärnutzung klinischer Daten in datensammelnden, nicht-interventionellen Forschungs- oder Lernaktivitäten – Begriff, Studientypen und ethische Herausforderungen. In: Richter G, Loh W, Buyx A, Graf von Kielmansegg S (eds.): Datenreiche Medizin und das Problem der Einwilligung: Ethische, rechtliche und sozialwissenschaftliche Perspektiven, 1st ed. Berlin, Heidelberg: Springer Berlin Heidelberg 2022; 71–98.
22. Sweeney L: Only You, Your Doctor, and Many Others May Know. https://techscience.org/a/2015092903/ (last accessed on 26 July 2022).
23. Blaser J: Herausforderungen der digitalen Medizin. Praxis 2018; 107(13): 712–6.
24. Deutscher Ethikrat: Big Data und Gesundheit: Datensouveränität als informationelle Freiheitsgestaltung. Berlin 2017.
25. Deutsches Ärzteblatt: Tausende Datensätze von Patienten in Berliner Krankenhaus gestohlen. https://www.aerzteblatt.de/nachrichten/108969/Tausende-Datensaetze-von-Patienten-in-Berliner-Krankenhaus-gestohlen (last accessed on 30 May 2022).
26. Bahners R: „medileaks.cc": Der größte bisher bekannte Datenklau im Gesundheitswesen. https://www.medical-tribune.de/praxis-und-wirtschaft/ehealth/artikel/medileaks-cc-der-groesste-bisher-bekannte-datenklau-im-gesundheitswesen/ (last accessed on 30 May 2022).
27. McCandless D, Evans T: World's Biggest Data Breaches & Hacks. Information is Beautiful. https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/ (last accessed on 30 May 2022).
28. Helm T: Revealed: how drugs giants can access your health records. https://www.theguardian.com/technology/2020/feb/08/fears-over-sale-anonymous-nhs-patient-data (last accessed on 21 June 2022).
29. Zentrale Ethikkommission bei der Bundesärztekammer: Entscheidungsunterstützung ärztlicher Tätigkeit durch Künstliche Intelligenz. Dtsch Arztebl 2021; 118(33–34): A-1537 / B-1277.
30. Mazzocchi F: Could Big Data be the end of theory in science? A few remarks on the epistemology of data-driven science. EMBO Rep 2015; 16(10): 1250–5.
31. Anderson C: The End of Theory: The Data Deluge Makes the Scientific Method Obsolete. https://www.wired.com/2008/06/pb-theory/ (last accessed on 21 September 2022).
32. Boyd D, Crawford K: CRITICAL QUESTIONS FOR BIG DATA: Provocations for a cultural, technological, and scholarly phenomenon. Information, Communication & Society 2012; 15(5): 662–79.
33. Rudinow Sætnan A: The haystack fallacy, or why Big Data provides little security. In: Rudinow Sætnan A, Schneider I, Green N (eds.): The Politics and Policies of Big Data: Big Data, Big Brother? London, New York: Routledge 2018; 21–38.
34. Caliebe A, Leverkus F, Antes G, Krawczak M: Does big data require a methodological change in medical research? BMC Med Res Methodol 2019; 19(1): 125.
35. Caliebe A, Burger H-U, Knoerzer D, Kieser M: Big Data in der klinischen Forschung: Vieles ist noch Wunschdenken. Dtsch Arztebl 2019; 116(35–36): A 1534–9.
36. Hemkens LG, Juszczak E, Thombs BD: Reporting transparency and completeness in trials: Paper 1: Introduction – Better reporting for disruptive clinical trials using routinely collected data. J Clin Epidemiol 2022; 141: 172–4.
37. Kwakkenbos L, Imran M, McCall SJ, et al.: CONSORT extension for the reporting of randomised controlled trials conducted using cohorts and routinely collected data (CONSORT-ROUTINE): checklist with explanation and elaboration. BMJ 2021; 373: n857.
38. Heinrichs B: Forschung am Menschen: Elemente einer ethischen Theorie biomedizinischer Humanexperimente. Berlin, New York: De Gruyter 2006.
39. Lanzerath D: Krankheit und ärztliches Handeln: Zur Funktion des Krankheitsbegriffs in der medizinischen Ethik. Freiburg Breisgau, München: Alber 2000.
40. Köngeter A, Schickhardt C, Jungkunz M, Bergbold S, Mehlis K, Winkler EC: Patients' Willingness to Provide Their Clinical Data for Research Purposes and Acceptance of Different Consent Models: Findings From a Representative Survey of Patients With Cancer. Journal of Medical Internet Research 2022; 24(8): e37665.
41. Köngeter A, Schickhardt C, Jungkunz M, Mehlis K, Winkler EC: Physicians' Attitudes towards Secondary Use of Clinical Data for Biomedical Research Purposes in Germany. Results of a Quantitative Survey 2022.
42. Lidz CW, Appelbaum PS: The therapeutic misconception: problems and solutions. Med Care 2002; 40(9 Suppl): V55–63.
43. Hoeyer K, Wadmann S: 'Meaningless work': How the datafication of health reconfigures knowledge about work and erodes professional judgement. Economy and Society 2020; 49(3): 433–54.
44. Ploug T: In Defence of informed consent for health record research – why arguments from ‚easy rescue', ‚no harm' and ‚consent bias' fail. BMC Med Ethics 2020; 21(1): 75.
45. Sachverständigenrat zur Begutachtung der Entwicklung im Gesundheitswesen: Digitalisierung für Gesundheit: Ziele und Rahmenbedingungen eines dynamisch lernenden Gesundheitssystems: Gutachten 2021. Bern: Hogrefe Verlag 2021.
46. Rheinsberg Z, Parsa-Parsi R, Wiesing U: Deklaration von Taipeh: Weltärztebund betont Nutzen von Gesundheitsdaten- und Biobanken. Dtsch Arztebl 2017; 114(46): A-2146 / B-1800 / C-1758.
47. Council for International Organizations of Medical Sciences (CIOMS): International ethical guidelines for health-related research involving humans. https://cioms.ch/wp-content/uploads/2017/01/WEB-CIOMS-EthicalGuidelines.pdf (last accessed on 30 May 2022).
48. Wiertz S: Die zeitliche Dimension des Broad Consent. https://doi.org/10.1007/s00481–022–00715–9 (last accessed on 21 September 2022).
49. Council of Europe: Recommendation CM/Rec(2016)6 of the Committee of Ministers to member States on research on biological materials of human origin. https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168064e8ff (last accessed on 9 February 2023).
50. Richter G, Buyx A: Breite Einwilligung (broad consent) zur Biobank-Forschung – die ethische Debatte. Ethik Med 2016; 28(4): 311–25.
51. Caulfield T: Biobanks and Blanket Consent: The Proper Place of the Public Good and Public Perception Rationales. King's Law Journal 2007; 18(2): 209–26.
52. Bundesärztekammer, Kassenärztliche Bundesvereinigung: Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis. Dtsch Arztebl 2018; 115(10): A-453 / B-395 / C-395.
53. Ploug T, Holm S: Eliciting meta consent for future secondary research use of health data using a smartphone application – a proof of concept study in the Danish population. BMC Med Ethics 2017; 18(1): 51.
54. Bundesministerium für Gesundheit (BMG): Wissenschaftliches Gutachten „Datenspende" – Bedarf für die Forschung, ethische Bewertung, rechtliche, informationstechnologische und organisatorische Rahmenbedingungen. https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/5_Publikationen/Ministerium/Berichte/Gutachten_Datenspende.pdf (last accessed on 9 September 2022).
55. Jungkunz M, Köngeter A, Spitz M, et al.: Stellungnahme zur Etablierung der sekundären Forschungsnutzung von Behandlungsdaten in Deutschland: Ergebnisse des Verbundprojekts LinCDat: „Learning from Clinical Data. Ethical, Social and Legal Aspects" 2022. doi:10.11588/fmk.2022.1.91697.
56. acatech – Deutsche Akademie der Technikwissenschaften: TechnikRadar 2022: Was die Deutschen über Technik denken. https://www.acatech.de/publikation/technikradar-2022/ (last accessed on 18 October 2022).

57. Bertelsmann Stiftung: Opt-out-Modelle für die Elektronische Patientenakte aus datenschutzrechtlicher Perspektive. https://www.bertelsmann-stiftung.de/de/publikationen/publikation/did/opt-out-modelle-fuer-die-elektronische-patientenakte-aus-datenschutzrechtlicher-perspektive (last accessed on 22 September 2022).
58. Nordfalk F, Hoeyer K: The rise and fall of an opt-out system. Scand J Public Health 2020; 48(4): 400–4.
59. Hoeyer K: Data as promise: Reconfiguring Danish public health through personalized medicine. Soc Stud Sci 2019; 49(4): 531–55.
60. Hoeyer K: Data paradoxes: The politics of intensified data sourcing in contemporary healthcare. Cambridge, Massachusetts: The MIT Press 2023.
61. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz, DSK): Petersberger Erklärung zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung. https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/DSKEntschliessungen/104DSK-Petersberger-Erklaerung.pdf?__blob=publicationFile&v=1 (last accessed on 8 February 2023).
62. Schneider I: Datentreuhandschaft durch Intermediäre: Chancen, Herausforderungen und Implikationen. In: Verbraucherzentrale NRW e. V. (ed.): Zu treuen Händen? Verbraucherdatenschutz und digitale Selbstbestimmung 2022.
63. Hardinges J: Defining a 'data trust'. https://theodi.org/article/defining-a-data-trust/ (last accessed on 21 June 2022).
64. Datenethikkommission der Bundesregierung: Gutachten der Datenethikkommission. https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf (last accessed on 21 September 2022).
65. Temperton J: NHS care.data scheme closed after years of controversy. https://www.wired.co.uk/article/care-data-nhs-england-closed (last accessed on 30 May 2022).
66. Vezyridis P, Timmons S: Understanding the care.data conundrum: New information flows for economic growth. Big Data & Society 2017; 4(1): 205395171668849.
67. Presser L, Hruskova M, Rowbottom H, Kancir J: Care.data and access to UK health records: patient privacy and public trust. https://techscience.org/a/2015081103/ (last accessed on 21 September 2022).
68. Powles J, Hodson H: Google DeepMind and healthcare in an age of algorithms. Health Technol 2017; 7(4): 351–67.
69. Carter P, Laurie GT, Dixon-Woods M: The social licence for research: why care.data ran into trouble. J Med Ethics 2015; 41(5): 404–9.
70. Vezyridis P, Timmons S: Resisting big data exploitations in public healthcare: free riding or distributive justice? Sociol Health Illn 2019; 41(8): 1585–99.
71. Sterckx S, Rakic V, Cockbain J, Borry P: „You hoped we would sleep walk into accepting the collection of our data": controversies surrounding the UK care.data scheme and their wider relevance for biomedical research. Med Health Care Philos 2016; 19(2): 177–90.
72. Copeland R: Google's 'Project Nightingale' Gathers Personal Health Data on Millions of Americans: Search giant is amassing health records from Ascension facilities in 21 states; patients not yet informed. https://www.wsj.com/articles/google-s-secret-project-nightingale-gathers-personal-health-data-on-millions-of-americans-11573496790 (last accessed on 27 July 2022).
73. Marelli L, Testa G, Hoyweghen I van: Big Tech platforms in health research: Repurposing big data governance in light of the General Data Protection Regulation's research exemption. Big Data & Society 2021; 8(1): 20539517211018783.
74. Ostherr K: Artificial Intelligence and Medical Humanities. Journal of Medical Humanities 2022; 43(2): 211–32.
75. Hurtz S: Project Nightingale: 50 Millionen Patientendaten landen auf Googles Servern. https://www.sueddeutsche.de/digital/google-project-nightingale-gesundheitsdaten-ascension-1.4681463 (last accessed on 22 November 2022).
76. Brownsword R: Regulating Automated Healthcare and Research Technologies: First Do No Harm (to the Commons). In: Laurie G, Dove E, Ganguli-Mitra A, McMillan C, Postan E, Sethi N et al. (eds.): The Cambridge Handbook of Health Research Regulation: Cambridge University Press 2021.
77. Muller SHA, Kalkman S, Thiel GJMW van, Mostert M, Delden JJM van: The social licence for data-intensive health research: towards co-creation, public value and trust. BMC Med Ethics 2021; 22(1): 110.
78. Breidenbach C, Sibert NT, Wesselmann S, Kowalski C: Die Beratung durch Ethikkommissionen bei einer multizentrischen Beobachtungsstudie in Deutschland – Aufwand und Kosten. Gesundheitswesen 2021; 83(8–09): 639–44.
79. Kraus M, Nauck M, Stahl D, et al.: Studienübergreifende Harmonisierung datenschutzrechtlicher und ethischer Gesichtspunkte in Patientenunterlagen: Eine Praxisanalyse. In: Richter G, Loh W, Buyx A, Graf von Kielmansegg S (eds.): Datenreiche Medizin und das Problem der Einwilligung: Ethische, rechtliche und sozialwissenschaftliche Perspektiven, 1st ed. Berlin, Heidelberg: Springer Berlin Heidelberg 2022; 167–184.
80. Bundesärztekammer: Verfahrensvorschlag zur Harmonisierung der berufsrechtlichen Beratung gemäß § 15 MBO-Ä. https://www.bundesaerztekammer.de/fileadmin/user_upload/_old-files/downloads/pdf-Ordner/MuE/2020–01–17_Verfahrensvorschlag.pdf (last accessed on 18 October 2022).
81. Martani A, Hummel P: Eine neue Generation des Datenschutzes? Gegenwärtige Unvollständigkeit, mögliche Lösungswege und nächste Schritte. In: Richter G, Loh W, Buyx A, Graf von Kielmansegg S (eds.): Datenreiche Medizin und das Problem der Einwilligung: Ethische, rechtliche und sozialwissenschaftliche Perspektiven, 1st ed. Berlin, Heidelberg: Springer Berlin Heidelberg 2022; 27–54.
82. Schneble CO, Elger BS, Shaw DM: Google's Project Nightingale highlights the necessity of data science ethics review. EMBO Mol Med 2020; 12(3): e12053.
83. Knudsen C, Bertelsen PS: Data Work in Health Care: The Case of Medical Secretaries. Stud Health Technol Inform 2021; 286: 60–4.
84. Taupitz J: Biobanken: Forschungsprivilegien im Datenschutzrecht. In: Katzenmeier C (ed.): Festschrift für Dieter Hart: Medizin – Recht – Wissenschaft. Berlin, Heidelberg: Springer 2020; 603–625.
85. Dierks C, Roßnagel A: Sekundärnutzung von Sozial- und Gesundheitsdaten – Rechtliche Rahmenbedingungen. Berlin: MWV Medizinisch Wissenschaftliche Verlagsgesellschaft 2019.
86. Schneider UK: Sekundärnutzung klinischer Daten – rechtliche Rahmenbedingungen. Berlin: MWV Medizinisch Wissenschaftliche Verlagsgesellschaft 2015.
87. Weichert T: Datenschutzrechtliche Rahmenbedingungen medizinischer Forschung: Vorgaben der EU-Datenschutz-Grundverordnung und national geltender Gesetze. Berlin: MWV Medizinisch Wissenschaftliche Verlagsgesellschaft 2022.
88. Frenzel. In: Paal/Pauly, DS-GVO BDSG, 3. Auflage 2021, DS-GVO Art. 9 Rn. 15, 108, 110.
89. Schaar K: Anpassung von Einwilligungserklärungen für wissenschaftliche Forschungsprojekte: Die informierte Einwilligung nach der DS-GVO und den Ethikrichtlinien. http://www.scientificdata.de/images/Artikel/ZD-05–2017---Beitrag-Schaar.pdf (last accessed on 22 September 2022).
90. Hänold S: 9. Nationales Biobanken-Symposium 2020 – Neue Entwicklungen zum „Broad Consent" in der medizinischen Forschung. ZD-Aktuell 2021: 5016.
91. Cepic M: Broad Consent: Die erweiterte Einwilligung in der Forschung. ZD-Aktuell 2021; 10: 5214.
92. Hänold S: Die Zulässigkeit eines „broad consent" in der medizinischen Forschung – a never ending story? ZD-Aktuell 2020: 6954.
93. Raum. In: Ehmann/Selmayr, DSGVO, 2. Aufl. 2018, Art. 89 Rn. 35.
94. Taupitz J, Schreiber M: Biobanken – zwischen Forschungs- und Spenderinteressen. Bundesgesundheitsblatt Gesundheitsforschung Gesundheitsschutz 2016; 59(3): 304–10.
95. Fröhlich W, Spiecker I: Die breite Einwilligung (Broad Consent) in die Datenverarbeitung zu medizinischen Forschungszwecken – der aktuelle Irrweg der MII. GesundheitsRecht 2022; 21(6): 346–53.
96. Deutscher Bundesrat: Gesetzentwurf der Bundesregierung. Entwurf eines Gesetzes zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur: (Patientendaten-Schutz-Gesetz – PDSG). BR-Drs. 164/20. https://www.bundesrat.de/SharedDocs/drucksachen/2020/0101–0200/164–20.pdf?__blob=publicationFile&v=1 (last accessed on 22 September 2022).
97. Deutscher Bundestag: Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz – PDSG) 2020.
98. Di Fabio. In: Dürig/Herzog/Scholz, Grundgesetz-Kommentar, Werkstand: 96. EL November 2021, Art. 2 Abs. 1 Rn. 175.
99. Guckelberger. In: Gersdorf/Paal, BeckOK Informations- und Medienrecht, 36. Edition Stand: 01.05.2022, § 5 IFG Vorbem.
100. Spindler/Dalby. In: Spindler/Schuster, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 9 DS-GVO Rn. 22 ff.
101. Frenzel. In: Paal/Pauly, DS-GVO, 3. Aufl. 2021, Art. 5 Rn. 32.
102. Weidemann. In: BeckOK StGB.
103. Dochow C: Unterscheidung und Verhältnis von Gesundheitsdatenschutz und ärztlicher Schweigepflicht (Teil 1). MedR 2019; 37(4): 279–87.
104. Deutscher Bundestag: Beschlussempfehlung und Bericht des Ausschusses für Gesundheit (14. Ausschuss) zu dem Gesetzentwurf der Bundesregierung – Drucksachen 19/18793, 19/19365, 19/19655 Nr. 3 – Entwurf eines Gesetzes zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz – PDSG): BT-Drs. 19/20708. https://dserver.bundestag.de/btd/19/207/1920708.pdf (last accessed on 22 September 2022).
105. Europäisches Parlament und Rat der Europäischen Union: Verordnung (EU) 2022/868 des Europäischen Parlaments und Rates über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724: (Daten-Governance-Rechtsakt) 2022.
106. Europäische Kommission: Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über den europäischen Raum für Gesundheitsdaten. https://eur-lex.europa.eu/resource.html?uri=cellar:dbfd8974-cb79–11ec-b6f4–01aa75ed71a1.0003.02/DOC_1&format=PDF (last accessed on 23 September 2022).

Members of the Central Ethics Commission
Prof. Dr. theol. Franz-Josef Bormann, Tübingen
Prof. Dr. jur. Frauke Brosius-Gersdorf, LL.M., Potsdam
Prof. Dr. theol. Elisabeth Gräb-Schmidt, Tübingen
Prof. Dr. med. Wolfram Henn, Homburg
Prof. Dr. (TR) Dr. phil. et med. habil. Ilhan Ilkilic, M.A., Istanbul/TR
Dr. phil. Julia Inthorn, Hanover
Prof. Dr. med. Dipl.-Soz. Tanja Krones, Zurich/CH
Prof. Dr. phil. Dirk Lanzerath, Bonn (Coordinator)
Prof. Dr. jur. Dr. h. c. Volker Lipp, Göttingen
Prof. Dr. med. Georg Marckmann, MPH, Munich
Dr. med. Stephan M. Probst, Bielefeld
Prof. Dr. med. Dr. phil. Sabine Salloch, Hanover
Prof. Dr. med. Jan Schildmann, Halle (Saale)
Prof. Dr. phil. Ingrid Schneider, Hamburg (Coordinator)
Prof. Dr. jur. Jochen Taupitz, Mannheim (Chair)
Prof. Dr. med. Dr. phil. Eva Winkler, Heidelberg

Expert Testimonies
Prior to the drafting this Opinion, an expert hearing was held with

- Lena Dimde, produkt manager ePA, gematik GmbH
- Dr. rer. nat. Johannes Drepper, research consultant, TMF e.V.
- Dr. rer. nat. Steffen Heß, Head of Health Research Data Centre, BfArM
- Prof. Klaus Hoeyer, Department of Public Health, Centre for Medical Science and Technology Studies, University of Copenhagen

The participants of the expert hearing are not authors of the Opinion and were not involved in the further elaboration of the Opinion. The Opinion does not necessarily reflect the opinions of the experts or their institutions.

Correspondence address
Zentrale Ethikkommission bei der Bundesärztekammer
Herbert-Lewin-Platz 1, 10623 Berlin
E-Mail: zeko@baek.de
https://www.zentrale-ethikkommission.de