

Code of Conduct for Health Research

Dealing responsibly with (personal) data and human tissue in Dutch health research

January 2022

English translation published in June 2023

This Code of Conduct is issued under the responsibility of the Committee on Regulation of Health Research, the [COREON Foundation](#).

The Code of Conduct came about through an extensive process of consultation. See **Appendix B** for more information on the process.

The text of the Code of Conduct is based on regulations as they apply on 1-1-2022. The Board of COREON thanks all those who have contributed to this Code of Conduct, including the members of the Sounding Board, COREON participants and the parties who contributed to consultations. In particular, the Board would like to thank the members and the Chair of the Core Group and the MCLF team that prepared the drafts and finalised the final texts.

The original text of the Code of Conduct is in Dutch. MLCF prepared this English translation as a service to the research community. The translation was subsequently reviewed by a professional translator under the coordination of Lygature (portfolio Health Law, Privacy and Ethics) on behalf of COREON as part of the implementation of the Code of Conduct. All the legal terms and main concepts of this Code of Conduct are consistently translated and, when applicable, use the terms of the GDPR.

The Code of Conduct on Health Research was made possible by financial contributions from:



Contents

Abbreviations	9
Definitions	11
Part 1: Code of Conduct.....	18
Introduction.....	19
Objective.....	19
Scope 20	
Target groups.....	21
Comments on the content, application and scope of the Code of Conduct	22
Reading guide	24
The main concepts.....	24
Explanation of the roles in the data processing chain	27
Structure of the Code of Conduct	29
1 Research design.....	32
1.1 Research protocol and data management plan	32
1.2 Anticipating follow-up activities for data protection	34
1.3 Review, notification and implementation of data protection impact assessment (DPIA)....	34
1.4 Responsibilities for institutions	36
2 Appropriate safeguards	38
2.1 Data minimisation	38
2.2 Data protection when providing	39
2.3 Prohibition on reidentification	40
2.4 Processing of directly identifying personal data	40
2.5 Access control.....	41
2.6 Responsibilities for institutions	41
3 Informing data subjects	44
3.1 Informing data subjects about data processing	44

3.2	Exemptions to the principle of informing by the research institution	46
3.3	Information and control of provision for secondary use: responsibilities of the provider ...	47
4	Conditions for research involving the collection of new data and human tissue from participants	48
4.1	Approaching potential participants.....	48
4.2	Explicit prior consent to data processing	50
4.3	Informed consent	52
4.4	Specific authorisation	53
4.5	Further specification of consent in the case of wide-ranging research	56
4.6	Freely granted consent.....	57
4.7	Demonstrable consent	58
4.8	Withdrawal of consent	58
5	Conditions for secondary use	60
5.1	Provision and secondary use of anonymous or anonymised data and human tissue	61
5.2	Conditions for secondary use of special category data: consent as the starting point	61
5.3	General consent for healthcare providers	62
5.4	Exemptions to the principle of consent for special category data.....	64
5.5	Conditions of secondary use on the basis of general consent or an exemption to the principle of consent	66
5.6	Provider responsibilities: control of provision for secondary use.....	67
5.7	Provider responsibilities: institutional policy on secondary use	68
6	Rights of participants with regard to data and human tissue	71
6.1	Exercise of rights: when and through which party?	71
6.2	Right of access	72
6.3	Right to rectification	72
6.4	Right of erasure	73
6.5	Right to data portability	73
6.6	Right to object	74
6.7	Dealing with individual findings.....	74

6.8	Responsibilities for institutions	75
7	Publication	76
7.1	Publish the results of research	76
7.2	Publishing information about patients or participants	76
7.3	Disclosure of research data	77
8	Management and archiving.....	79
8.1	Safeguarding responsibility for management	79
8.2	Defining retention periods	79
8.3	Appropriate safeguards for archiving.....	80
8.4	Responsibilities for institutions	81
9	Use and re-use of research data and human tissue for new research.....	82
9.1	Anticipating use and re-use for future research	82
9.2	Complying with data protection rules for use and re-use in new research	83
10	Controllershship.....	85
10.1	Main rule: when does one become a data controller?	85
10.2	Joint controllers	86
10.3	Processors.....	88
10.4	Securing distinction between different roles within one organisation.....	90
10.5	Defining roles in agreements.....	91
11	Assurance, monitoring and implementation	92
11.1	Security	92
11.2	Monitoring compliance with the Code of Conduct	93
11.3	Implementation and further development	93
	Part 2: Legal foundation	95
	Explanation of the legal justification	96
	Introduction.....	97
	Purposes	98
	Scope	98

Target groups.....	100
Comments on the content, application and scope of the Code of Conduct	100
Reading guide	102
1 Research design.....	107
1.1 Research protocol and data management plan	107
1.2 Anticipating follow-up activities for data protection	109
1.3 Review, notification and implementation of data protection impact assessment (DPIA) ..	109
1.4 Responsibilities for institutions	110
2 Appropriate safeguards	111
2.1 Data minimisation	111
2.2 Data protection when providing	111
2.3 Prohibition on reidentification	113
2.4 Handling of directly identifying personal data	113
2.5 Access Security	113
2.6 Responsibilities for institutions	114
3 Informing data subjects	115
3.1 Informing data subjects about data processing	115
3.2 Exemptions to the principle of information provision by the research institution.....	115
3.3 Information and control of disclosure for secondary use: provider responsibilities	116
4 Conditions for research involving the collection of new data and human tissue from participants	117
4.1 Approaching potential participants.....	117
4.2 Express prior consent to data processing.....	120
4.3 Informed consent	122
4.4 Specific authorisation	122
4.5 Further specification of consent in the case of wide-ranging research	124
4.6 Freely granted consent.....	125
4.7 Demonstrable consent	126

4.8	Withdrawal of consent	126
5	Conditions for secondary use	128
5.1	Provision and secondary use of anonymous or anonymised data and human tissue	129
5.2	Conditions for secondary use of special category data: consent as the starting point	130
5.3	General consent for healthcare providers	130
5.4	Exemptions to the principle of consent for special category data	133
5.5	Conditions for secondary use on the basis of general consent or an exemption to the consent principle	134
5.6	Provider responsibilities: control of provision for secondary use	135
5.7	Provider responsibilities: institutional policy on secondary use	135
6	Rights of participants with regard to data and human tissue	137
6.1	Exercise of rights: when and through which party	137
6.2	Right of access	138
6.3	Right to rectification	138
6.4	Right to erasure	138
6.5	Right to data portability	139
6.6	Right to object	139
6.7	Dealing with individual findings	140
7	Publication	141
7.1	Publishing the results of research	141
7.2	Publishing information about patients or participants	141
7.3	Disclosure of research data	142
8	Management and archiving	143
8.1	Securing responsibility for management	143
8.2	Defining retention periods	144
8.3	Appropriate safeguards for archiving	145
8.4	Responsibilities for institutions	145
9	Use and re-use of research data and human tissue for new research	147

9.1	Anticipating use and re-use for future research	147
9.2	Complying with data protection rules when used and re-used in new research	148
10	Controllershship.....	149
10.1	Main rule: when controller.....	149
10.2	Joint controllers.....	149
10.3	Processors.....	152
10.4	Securing distinction between different roles within one organisation.....	152
10.5	Defining roles in agreements.....	153
11	Assurance, monitoring and implementation	154
11.1	Security.....	154
11.2	Monitoring compliance with the Code of Conduct	154
12	References	155
	Appendix A: Overview of relevant legal articles per section.....	159
	Appendix B: Establishment of the Code of Conduct	161

Abbreviations

Abbreviation	Meaning
AP	Dutch Data Protection Authority
CBS	Central Bureau of Statistics
CCMO	Central Committee on Research involving Human Subjects
DAC	Data Access Committee
DPIA	Data Protection Impact Assessment
ECTR	European Clinical Trial Regulation
EDPB	European Data Protection Board
EU	European Union
FAIR	Findable, accessible, interoperable, reusable
DPO	Data Protection Officer
GDPR	General Data Protection Regulation
IGJ	Health and Youth Care Inspectorate
MEC	Medical Ethics Review Committee
NEN	Royal Netherlands Standardization Institute
nWMO	Not subject to WMO (the Medical Research Involving Human Subjects Act)
TTP	Trusted third party
UAVG	Dutch General Data Protection Regulation Implementing Act
UMC	University Medical Centre

Wgbo	Act on the medical treatment agreement
WMO	Medical Research Involving Human Subjects Act
WODC	Scientific Research and Documentation Centre
Wzi	Human Tissue Control Bill

Definitions

Term	Definition	Origin
Administrator	Legal person or, in the absence of a legal person, the individual who stores, provides or transfers data or human tissue with a view to its use or future use.	Art. 1 WzI
Anonymisation	Processing personal data in such a way that it subsequently ceases to be personal data.	Derived from Recital 26 GDPR
Basis (legal basis)	The legal ground that justifies a data processing operation.	Particularly important here are Articles 6 and 9 GDPR and Articles 7:457 and 7:458 of the Civil Code.
Care provider	An institution or a solo practitioner.	Art. 1.1 Wkkgz
Coded data	Data in which directly identifying data to distinguish the participants have been replaced by a code number. This can be pseudonymised data within the meaning of the GDPR, or coded data that is not pseudonymised data within the meaning of the GDPR. The coding must be reproducible at the provider.	This Code of Conduct
Communication data	Data that can be used to contact the participant. Communication data are always directly identifying data.	

Consent as a basis for data processing under the GDPR ('GDPR consent')	Any freely given, specific, informed and unambiguous expression of will by which the data subject accepts, by declaration statement or unambiguous active action, the processing of personal data relating to him or her.	Art. 7 GDPR, EDPB Guideline 05/2020 on consent under Regulation 2016/679
Controller	A natural or legal person, public authority, agency or any other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union law or Member State law, the latter may determine who the controller is or how the controller is designated.	Art. 4.7, 24 GDPR
Data management plan	The plan describing how research data will be handled both during and after the research.	This Code of Conduct
Data minimisation	Data processing in such a way that personal data are adequate, relevant and limited to what is necessary for the purposes for which they are processed.	Art. 5.1c GDPR
Data Protection Impact Assessment (DPIA)	An assessment of the impact of an intended processing activity on the protection of personal data. The result of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate compliance with the GDPR when processing personal data.	Art. 35 - 36 GDPR
Data Protection Officer (DPO)	Person who supervises compliance with the GDPR within an organisation.	Art. 37 - 39 GDPR
Data subject	An identified or identifiable individual to whom the data concerned relates. A data subject is also a	Art. 4.1 GDPR

	'participant' if his/her human tissue and/or data are involved in scientific research.	
Directly identifying data	Personal data that can be traced directly to a natural person without additional data.	Derived from Recital 26 and Art. 4.1 GDPR
Donor	Human source of available human tissue, in the form of a living or deceased person or stillborn.	Art. 1 Wzl
Future scientific research	Research for which the research questions are not yet fully known or specified at the time of processing for research purposes (collection or processing of data or collection of human tissue).	This Code of Conduct, Wzl
General consent	Giving consent on the basis of general information about what the research entails in order to breach medical confidentiality.	Derived from art. 7:457 Wgbo
Human tissue	Any substance, constituent or part separated from the donor.	Art. 1 Wzl
Indirectly identifying data	Personal data that can only be traced back to a natural person with additional data.	Derived from Recital 26 and Art. 4.1 GDPR
Individual findings	Individual research findings, which may be of direct significance for the health (current or future) of a particular participant/donor and/or blood relatives.	Art. 1 Wzl
One-way coded data	Data where the directly identifying data have been replaced by a code number and where there is no path (key) back from the coded data to the directly identifying data on which the code number is based, e.g. a one-way hash. See further under Coded data.	

Open data	Data that is accessible to everyone without restrictions.	
Participant	The generic term for a data subject whose data and/or human tissue are processed in scientific research. This can be a healthy volunteer or patient whose data are processed in research, but also a test subject in the sense of the WMO, or for example a donor in the sense of the Wzl.	This Code of Conduct
Personal data	All information about an identified or identifiable natural person. When data is qualified as personal data, the GDPR applies and a basis for the processing of that data is required, among other things.	Art. 4.1 GDPR
Processing	An operation or set of operations relating to personal data or a set of personal data, whether or not performed by automatic means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.	Art. 4.2 GDPR
Processor	A natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller. A processor <u>always works at the behest of a controller</u> , and thus can never independently determine the purposes and means of processing personal data.	Art. 4.8, 28 GDPR
Provider	The person (may be any natural or legal person) who provides data to the researcher for the purpose of scientific research without being a	This Code of Conduct

	<p>participant himself. A provider is always linked to a data controller or is the controller him/herself. Provision can take place within the institution of the person responsible for processing, namely from a care provider to the researcher or from one researcher to another researcher.</p>	
Pseudonymisation	<p>Processing of personal data in such a way that the personal data cannot be linked to a specific data subject without the use of additional data, provided that such additional data are stored separately and that technical and organisational measures are taken to ensure that the personal data are not linked to an identified or identifiable natural person.</p>	Article 4.5 GDPR
Pseudonymised data	<p>Data that have been pseudonymised (see definition of "pseudonymisation").</p>	
Research data	<p>All data collected during scientific research for the purpose of analysis according to the research protocol.</p> <p>Research data can be distinguished from communication data.</p>	
Research file	<p>The documents to be submitted to the Review Committee.</p>	
Research institution	<p>The data controller where research data is processed.</p>	This Code of Conduct
Research protocol	<p>The complete description of a proposed scientific study research including the objectives, design, methodology, statistical aspects and organisation of the scientific study.</p>	WMO, section 1, subsection d. Incidentally, the term is also used in health

		research outside the WMO
Re-use	Subsequent processing for scientific research of personal data and human tissue previously collected or processed for scientific research.	
Sampling protocol	The description of an intended special collection of human tissue for the purpose of scientific research (current or future). The sampling protocol contains, among other things, a description of the objectives of the scientific research to be performed with the human tissue, for example a subfield of medicine.	Derived from art. 16 WzI
Scientific research	Generating knowledge through systematic research and reflection, observation and experimentation that is in accordance with the relevant methodological and ethical standards of the sector, and conforms to good practice. Health research is also always scientific research.	This Code of Conduct
Secondary use	Processing for scientific research purposes of personal and human tissue that has been collected or processed primarily for another purpose. English near equivalent: ' <i>further use</i> '.	Derived from Art. 5.1b GDPR
Special category data	Sensitive personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the unique identification of an individual, data concerning health and/or data concerning a person's sexual behaviour or orientation.	Recitals 51-54 and Art. 9 GDPR

Special privacy risks and consequences	Individual consequences for participants that do not fall within the reasonable expectations people have about health research.	This Code of Conduct
Test subject	Person subjected to a certain action or having a certain behaviour imposed in the context of scientific research.	WMO
Trusted Third Party	An independent party that acts as an intermediary for the exchange of data between two or more parties, and is responsible for the coding of personal data.	Derived from NEN norm 7524

Part 1

Code of Conduct

Introduction

Health research is of great and increasing social importance. It contributes to new insights into disease and health, to the prevention and improvement of healthcare, and to the development and implementation of (bio)medical innovations. In the past decade, it has gained in importance, both qualitatively - for instance in the development towards 'personalised' or 'precision medicine' - and quantitatively, also in large international research groups.

For such research, much data, images and human tissue, mostly sensitive, from many participants are processed. By participating in research, this contributes to a better perspective on health, cure and future treatments, and to better care and public health. A large majority of patients and citizens are generally positive about health research.¹ However, they expect their personal data and human tissue to be processed safely and carefully, with respect for their rights and interests.

Objective

The legislation and regulations for data protection in health research are complex and are partly based on general, open standards which need to be further specified for application in practice. The present code of conduct elaborates them into a set of concrete standards for Dutch health research that is accessible to researchers. The process of development is explained in [Appendix B](#). During the elaboration process the aim was to ensure that these standards:

- are legally conclusive according to European and Dutch law;
- are ethically justified; *and*
- are as workable as possible for researchers and research institutions.

The Code of Conduct aims to clarify which rules Dutch health research should comply with. A set of clear rules prevents researchers from applying different standards and institutions from testing health research against different standards. These differences stand in the way of good cooperation within Dutch health research.

The Code of Conduct also aims to contribute to the trust that citizens and patients should have in health research.

¹See amongst others the study by the Patiëntenfederatie, [Delen van uw data. hergebruik van gezondheidsgegevens en lichaamsmateriaal voor wetenschappelijk onderzoek](#), Utrecht, November 2019; Coppen R., Groenewegen P.P., Hazes J.M.W.M., et al. Hergebruik van medische gegevens voor onderzoek. What do Dutch people think of the consent requirement? *Ned Tijdschr Geneeskd.* 2015;160:A9868.

The General Data Protection Regulation (GDPR) is the primary source for the Code of Conduct. At the same time, it leaves room on a number of points for supplementary or special Dutch legislation. In addition to the Dutch GDPR Implementation Act (UAVG), rules laid down in the Medical Treatment Agreement Act (Wgbo) for the confidential handling of medical data are particularly important in this respect. Legislation on the control of human tissue and medical research involving it are currently being prepared (the future Human Tissue Control Act, WzI). The Code of Conduct elaborates them in conjunction.

Scope

The term 'health research' is interpreted broadly in this Code of Conduct. The following three elements are important in this context:

- Health research is *scientific* research. Scientific research aims to acquire knowledge by systematically collecting and studying data. Scientific research is intended to contribute to knowledge that is also valid for populations outside the direct research population.²
- *Health research* is all research that aims to answer questions in the areas of illness, health and healthcare. This includes research into the causes, backgrounds and models of illness and health, prevention and treatment methods, as well as the functioning of the health care system itself.
- *Various statutory frameworks* apply to health research within the meaning of this Code of Conduct. Health research therefore encompasses all research as defined in the Medical Research Involving Human Subjects Act (WMO) (research for which the WMO is mandatory). It also includes questionnaire and biobank research and secondary use. The latter is research that uses data and human tissue previously collected for other purposes, such as individual healthcare (research not subject to the WMO).

The scope of the Code of Conduct is broader than that of the GDPR in two respects.

- The GDPR relates only to the processing of *personal data of living persons*. In the Netherlands, however, medical confidentiality continues after death. A number of rules in the Wgbo and

² This interpretation is in line with the CCMO definition of medical research: <https://www.ccmo.nl/onderzoekers/publicaties/publicaties/2005/11/25/ccmo-notitie-definitie-medisch-wetenschappelijk-onderzoek>. Compare also the Dutch Code of Conduct for Scientific Integrity 2018, which defines scientific research as '*the quest for knowledge obtained through systematic study and thinking, observation and experimentation*'.

the future Wzl therefore also offer protection, to a certain extent, for previously collected data and human tissue *of deceased patients*.³ This is reflected in this Code of Conduct.

- The handling of *human tissue* in research is inextricably linked to the processing of personal data. Related questions concerning the protection of the rights and freedoms of individuals also play a role because human tissue usually contains personal data. Separate legislation - the aforementioned Wzl - is being prepared for this.⁴ The Code of Conduct takes this into account as much as possible. COREON also drew up a 'Code of conduct for the responsible use of bodily tissue in scientific research' (Code Goed Gebruik 2011). The present Code of Conduct, together with the Wzl, replaces this earlier code.

Careful data processing in the context of this code of conduct requires more than just researchers and other parties involved abiding by the rules of this code and the related legislation. In addition, the current standards of scientific integrity, ethical guidelines and general expectations of citizens, patients and participants regarding health research must be respected. The starting point is therefore that if this code of conduct is followed, the Dutch Code of Conduct for Scientific Integrity⁵ must also be followed. The reader's guide and substantiation further explain how scientific integrity standards are reflected in the Code of Conduct.

Target groups

Compliance with data protection law is formally the responsibility of the data controller. These are almost always the organisations (or their boards) to which researchers or healthcare workers are attached. The Code of Conduct is aimed at these responsible parties and describes per chapter the most important consequences of the standards that apply to researchers.

The standards of this Code of Conduct have been drawn up primarily for researchers, other professionals and institutions involved in the design, implementation and support of data processing and the use of human tissue for health research. In practice, they are the ones who are responsible for data protection. Clarity about the applicable regulations is of primary importance to them. By specifically addressing the researchers, the Code of Conduct also facilitates the practical implementation of the legal standards by the data controller.

³ Article 7:457 of the Civil Code.

⁴ Bill on rules for actions with human tissue performed for purposes other than medical treatment or diagnosis of the donor (Human Tissue Control Act), Parliamentary Papers 35844.

⁵ See the [Dutch Code of Conduct for Scientific Integrity](#).

In order to make the standards accessible to everyone, legal jargon has been avoided as much as possible. In a separate explanation, the standards are placed in the context of legislation and legal terminology, and the choices made are legally justified.⁶

Although the Code of Conduct is primarily aimed at researchers, it is also important for other parties.

- Review and assessment committees can use the Code of Conduct for the assessment of proposed research and the establishment of bio- and databanks.
- Regulators, such as the Personal Data Authority but also the Health and Youth Care Inspectorate, can use the Code of Conduct in their supervisory practice.
- Finally, the Code of Conduct provides clarity for citizens and patients on what they may expect from the handling of their data and human tissue when participating in health research.

Comments on the content, application and scope of the Code of Conduct

This code of conduct is not a systematic explanation of all norms of the relevant privacy regulations. It deals with the norms that are specifically relevant in the context of health research and that require further elaboration in concrete rules. This means that not all general norms from the GDPR about data processing that always apply to every data controller, even outside the context of health research, are reflected in this code.

The Code of Conduct is not a 'cookbook' or SOP (*standard operating procedure*). When applying the rules to a specific study or situation, further consideration will sometimes be involved. It is up to the researchers, institutions and other parties responsible for data processing to make responsible considerations, in line with the principles of the Code of Conduct. [Data protection officers](#) (DPOs), review committees, institutional lawyers and quality officers, among others, will assess these considerations.

In addition, the Code of Conduct does not address a number of specific subjects. An example is the rules for health research on incapacitated persons and minors under 16. The Code of Conduct suggests that the rules on representation in research not subject to the Medical Research (Human Subjects) Act should be aligned with the rules on representation in the Medical Research (Human Subjects) Act (Wgbo) (see [chapter 4](#)). At the same time, nuances are probably needed for research specifically aimed

⁶ See Part II.

at these groups (see also the legal basis). This may be addressed in a separate Code of Conduct. This is just one of the subjects within data protection in health research that requires further elaboration.

A number of subjects do not fall within the scope of this code of conduct. Quality registrations and the evaluation of quality of care also involve the secondary use of patient data, but this is subject to different legal conditions.⁷ Measurements and benchmarking for the purpose of quality control or evaluation – as often carried out by quality registries set up for this purpose – are not primarily intended for scientific health research as described in this Code of Conduct. Such activities are not aimed at acquiring knowledge outside the population from which data are processed, even if scientific methods are used. However, if personal data are processed for the purpose of scientific research, even if they were first collected for quality purposes, then this Code of Conduct does apply. Research carried out within the framework of care evaluation as supported by the Care Evaluation and Appropriate Use Programme therefore generally falls within the scope of the Code of Conduct.

This Code of Conduct does not take into account circumstances of scientific research in disciplines outside health research, such as those addressed by the ethical frameworks and review procedures for behavioural and social science research with humans established by Nethics.⁸ Nevertheless, many elements of data protection may apply accordingly. Other fields of science are of course free to make their own interpretation based on the rules of this Code of Conduct.

Finally, it should be noted that, despite a shared European legal framework for data protection, the rules for research involving personal data and human tissue may differ between countries. The GDPR explicitly leaves room for this. In this Code of Conduct, the Dutch laws and regulations have been elaborated within the general European framework. Deviating foreign regulations and possibilities for data processing for health research have not been taken into account. For cooperation within Europe, the main rule will be that the specific rules of the country of origin determine which data may be processed in which way in the international project. Special conditions apply to data exchange with countries outside the European Economic Area, such as the United States. These are not addressed in the Code of Conduct.

⁷ See, among others, the [preliminary draft of the Care Quality Registration Act](#).

⁸ National Ethics Consultation Social and Behavioural Sciences ([Nethics](#)).

Reading guide

When drawing up the standards, the aim was to make them as understandable and applicable as possible for researchers. For a proper understanding of the Code of Conduct, however, an explanation of a number of central, mostly legal concepts is necessary. These are explained below. Then the structure of the Code of Conduct is discussed. The further legal foundations are discussed in a separate section.

The main concepts

Health research always involves a shorter or longer chain of activities in which data and human tissue are collected, further processed and used for research.

It is always about:

1. data, in particular personal data, and human tissue (where appropriate).

That data comes from somewhere, in the context of the Code of Conduct from:

2. the participant and/or a provider.

Making personal data available for the purpose of health research is called:

3. provision.

The handling of personal data is called:

4. data processing.

This requires, among other things:

5. a basis or legal basis.

The authority that must have such a basis is called:

6. data controller.

The Code of Conduct names the data controller that processes personal data for the purpose of health research:

7. the research institution.

The numbered terms are explained below.

Personal data

Personal data is any data that in any way provides information about a specific, identifiable person. It can be [directly](#) or [indirectly identifying data](#). Directly identifying data can be used to directly identify a person. Indirectly identifying data can be used to reidentify a person by combining it with other data. These concepts apply by analogy to human tissue. Communication data of participants in research are an excellent example of directly identifying data.

Within the group of data, the Code of Conduct makes distinctions. 'Coded data' is the *umbrella* term for all data where participants can be distinguished by a separate number. That number replaces directly identifying data. With the code number, participants can still be distinguished.

Pseudonymised data is a special form of coded data. In this case, the provider has a key back to the participant's directly identifying data. The GDPR requires that this key is kept secure and separate from the other data. Coded data without a key back to the participant's identifying data, so-called 'one-way coded' data, are not pseudonymised data within the meaning of the GDPR, but they may still be personal data. See below under anonymous data.

Coding is an important security measure for the privacy of participants. That is why coding is of paramount importance in the Code of Conduct. Secure coding must meet a number of conditions (see [chapter 2](#)). Coding is also important if participants are to exercise their rights, for example if they withdraw their consent or make an objection. This must be passed on via the provider (see below) to the research file where the data is processed. This is elaborated on in [chapter 6](#).

In contrast to personal data, there are anonymous data. These are not covered by the GDPR. Coded data are considered personal data unless: this coding is irreversible, *and* the research data linked to the code cannot be traced back to the participant in any other way.

The line between personal and anonymous data is not always easy to draw. The question is what criteria apply to determine whether someone's identity can no longer be ascertained. This is a matter of debate. Is identification no longer reasonably possible, given all the circumstances under which the research data are processed? Or is it really no longer possible? Between these extremes there are nuances. The Code of Conduct does not take a stand on this. Suffice it to say that in health research,

the bar for anonymous data is set very high. Determining whether data are anonymous in a specific situation often requires statistical, legal and sometimes technical expertise.

This also means the following. If a researcher thinks he has 'anonymous' data at his disposal because they are encoded, this does not mean that they are anonymous in the sense of the GDPR. This mistake is often made by the researchers themselves (who rightly claim not to have any reason to identify) and subsequently in the information about the data processing. The Code of Conduct therefore advises only speaking of anonymous data if it can be reasonably assumed that the data are indeed anonymous (whether or not after consultation with the aforementioned experts).

Participant and provider

In health research, the data can come from:

- a. The *participant* himself (questionnaires, [human tissue](#)). The participant is the person whose data or human tissue is involved in [scientific research](#). In WMO terms the participant is a [test subject](#). The code of conduct uses participant as an umbrella term. In GDPR terms the participant is always a 'data subject'; *and/or*
- b. A [provider](#). This means a person or organisation that *can legitimately process* the data required for the research for a purpose other than scientific research (i.e. has a basis for this other purpose) and provides this data to the [research institution](#).

[Chapter 4](#) deals specifically with the conditions for health research when the personal data come directly from the participant. [Chapter 5](#) deals with the conditions when they come from a provider. Thus, the Code of Conduct also deals with the questions of when and how providers may make data available for health research.

Provision

To provide is to make data available for health research. This can be done through transfer, but also through data retention and access by the research institution.

Data processing

[Data processing](#) is anything that can be done with personal data, such as collection, storage and retention, use for analysis, and anonymisation.

Basis or legal basis

The *legal basis* or [basis](#) determines whether personal data may be processed at all (for example, because it is prescribed by law or because the [data subject](#) has given his or her consent). In the context of health research, two types of basis can be distinguished. The first is the general basis, which must always be met. The second is the special basis, which applies to the processing of special categories of personal data, such as data concerning health and genetic data.⁹

In chapters [4](#) and [5](#) these bases are specifically dealt with. It is important to note that a basis is a necessary, but not a sufficient condition to process personal data. The general principles of the GDPR must also be met. These are dealt with first in this Code of Conduct.

Controller

The [controller](#) is ultimately responsible for ensuring that the obligations of the GDPR are met. This is the body that determines the purpose and means of data processing. The legal definition is more detailed (see the glossary), but this is the essence. In the context of the Code of Conduct, the data controller is almost always a legal entity or an administrative body.

Sometimes it is difficult to determine who this controller is. Sometimes there are joint controllers. [Chapter 10](#) discusses this in more detail.

Research institution

The data made available are then sent to the research institution.

- The *research institution* is an organisation that processes data for scientific research. Researchers are attached to the research institution. This organisation can exclusively carry out research, but it can also have several purposes. For example, a University Medical Centre (UMC) has three goals: patient care, scientific research and education. If an organisation receives data for health research purposes, it is a research institute.

Explanation of the roles in the data processing chain

The GDPR only deals with the role of the data controller and its responsibilities towards the potential or existing participant. The roles distinguished in this Code of Conduct – namely provider and research institution – are more subtle.

⁹ Formally, this special basis in the GDPR is not a 'basis' but an exemption to a prohibition.

This is based on the following:

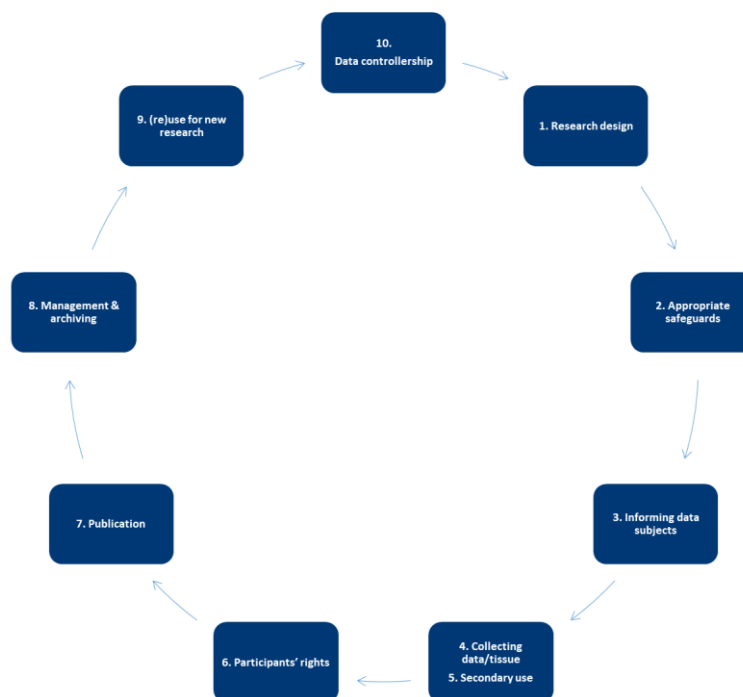
- These terms are in line with the terminology commonly used in health research;
- The provider may also be a healthcare professional, i.e. an individual associated with a [healthcare provider](#). That healthcare provider is the data controller, but the healthcare provider determines, within the boundaries of the law and its professional responsibilities, whether or not it provides data for health research;
- The research institute is always the data controller. This is usually a so-called legal entity, such as a private company or a foundation. In certain cases it can also be an individual, such as a doctor without a permanent contract, who initiates research himself. In general, however, the Code of Conduct considers it unlikely that an individual will meet the standards for a research institution.

It often happens that the provider is connected to the same organisation as the researcher. After all, the research institution can provide patient care as well as conduct research. The provision of data or human tissue by the provider to the researcher within the same organisation is also regarded as provision in the code of conduct. As a result of this internal provision, the organisation to which both (provider and researcher) are linked becomes a research institution.

The roles are not always exclusive. A research institution can also be a provider if it provides data to another research institution.

Structure of the Code of Conduct

The structure of the Code of Conduct broadly follows the 'data life cycle' of research and the steps that are typically followed: from design, through collection, analysis and management, to publication and possible re-use of data and human tissue. Different parts refer to each other and build on each other. This applies in particular to the design of the research. In the design, many aspects must be taken into account that will be addressed in the preparation and implementation. Where necessary, standards are elaborated or explained separately for a number of general forms of research. Standards that are directly aimed at the institutions involved are dealt with separately. The following diagram shows the structure of the part of the Code of Conduct that is aimed at the researchers. The numbering refers to the chapters.



The standards of the Code of Practice start with what, from a data protection perspective, should be taken into account when designing health research (chapter [1](#)).

Next comes the elaboration of the research. For a number of rules and principles, the GDPR leaves more room for scientific research than for other types of processing, provided that appropriate safeguards are in place (chapter [2](#)).

After an intermediate chapter on transparency in data processing that involves informing the data subjects ([chapter 3](#)), the further conditions for two types of research are discussed:

- 1) Research for which data and human tissue are specifically collected or taken from participants ([chapter 4](#)). This includes research to which the WMO applies and data processing for studies subject to the WMO, as well as survey research that is not subject to the WMO, or the special collection of human tissue for management in a biobank for future scientific research.
- 2) Research in which data and human tissue are processed that were previously collected for another purpose. Two situations can apply here:
 1. Secondary use of data collected in the context of the original purpose of the controller, such as individual healthcare by a care provider ([chapter 5](#)); *or*
 2. Re-use of data collected in the framework of research or stored in a research data/biobank for use in new research. By following the 'data life cycle', this is the last of the standards aimed at researchers to be handled ([chapter 9](#)).

The processing of data and human tissue for research often involves several parties in different roles. There is usually a chain of processing and collaboration in research involving the provider and the controller(s). It is important that it is clear who is responsible for which processes in the chain ([chapter 10](#)).

The controller(s) must also ensure that participants can exercise their rights in relation to data processing. [Chapter 6](#) discusses what those rights are and what data controllers must organise in that context.

[Chapter 7](#) deals with the standards for publishing the results of health research. This gives substance to general requirements of care for honest scientific research along with the principles of data protection, such as lawfulness, fairness and transparency.

Specific standards apply to the management and archiving of personal data and human tissue for scientific research. These include some storage restrictions, both during and after the research. These are discussed in [chapter 8](#).

The final section deals with the safeguarding, implementing and further development of this Code of Conduct as envisaged by the authors.

A separate section deals with the legal foundation. This part also explains in detail how the standards relate to, and elaborate on, the legal frameworks.

1 Research design

This chapter describes what should be considered when designing health research from a data protection perspective.

1.1 Research protocol and data management plan

1.1.1 Describe and justify the design of the study and the [processing](#) of data and human tissue required for it in a [research protocol](#) or a biobank or [collection protocol](#) (in the case of special collection of [human tissue](#) for [future scientific research](#)).

Provide a design that can answer the research question or achieve the research purposes. Provide a careful methodological foundation for this.

The importance of a research protocol for data protection

A sound research design and methodological foundation are not only important for the scientific quality of research. They are also important for responsible data protection, particularly for demonstrating that data processing is necessary to achieve the aims of the study (see in particular [chapter 2](#)). Depending on the research, this may involve a brief or comprehensive protocol. The Central Committee on Research Involving Human Subjects (CCMO) has made a [model protocol](#) available [for research that is subject to the WMO](#). Various institutions have their own model protocols for research that is not subject to the WMO.

1.1.2 Lay down concrete agreements about the management and processing of data and human tissue in the protocol or in a [data management plan](#). Do this before starting the collection and processing or as soon as possible afterwards.

The importance of a data management plan

A data management plan is usually based on standard terms and conditions, for example, institutional policy on data management. It can also be a living document that is further developed (with version management) as the research progresses. It is important that all aspects that are essential for legitimate processing – such as what the [participant](#) is informed about and for which consent is requested – are recorded prior to the start of processing. For examples and templates of data management plans, see [DMPonline](#).

Ensure that the research protocol and data management plan address:

- The purpose and methodology of the study, the collection and processing of data and human tissue;
- A schematic overview of the processing of data and/or human tissue, and the different processing steps envisaged. (Although this is not a formal requirement in the data protection rules, it often makes it clearer how the processing is organised and which parties are responsible for which parts of the processing. It is therefore strongly advised);
- The groups (categories) of [data subjects](#) whose data and/or human tissue are processed: who (which groups or populations) will participate in the study?;
- The types (categories) of data and/or human tissue being processed. In particular: are [special category data](#) processed? Are [directly identifying personal data](#) also processed? (See [chapter 2](#));
- Appropriate safeguards: How are only the data and human tissue necessary for the research processed in such a way that the amount of [data processed is minimal](#)? Is the data [coded](#) or [pseudonymised](#)? How is access to the data arranged? In which secure environment(s) are data processed? (see [chapter 2](#));
- The general conditions for processing and how they are implemented. How are participants approached and informed about the research? Will participants be asked for consent (and if so, how)? Or does an exemption apply (and if so, which one)? Or will only anonymised data be processed? (See [chapter 3](#) and [chapter 5](#));
- The division of [controllership](#): which parties are involved in the processing and in what role? (See [chapter 10](#));
- Dealing with participants' rights: which rights apply? Is there a chance of individual [findings](#) and how is this dealt with? (See [chapter 6](#));
- The management and archiving of data and human tissue: who is responsible? Which management regulations apply? (See [chapter 8](#));
- The retention period of collected data and/or human tissue: what retention period is applied and on what is it based? (See [chapter 8](#)); *and*
- The possibilities for and agreements on re-use, issue of and/or access to data and human tissue for future research. Is re-use foreseen? How will the FAIR principles of data management be implemented? How are decisions taken on requests for re-use, transfer or access? (See [chapter 9](#)).

For an explanation of the terms used and the conditions that apply, see the following chapters and the list of definitions.

1.2 Anticipating follow-up activities for data protection

1.2.1 When designing the study and/or collecting data and human tissue, take into account expected and unexpected issues that may require future attention from a data protection perspective.

These include:

- Informing participants after or during the study. This can be done, for example, through regular contact moments, newsletters or a research website (especially in the case of data collection and special collection of human tissue in long-term cohort studies, see [chapter 3](#) and [chapter 4](#));
- Rights of participants, procedures for their exercise, and participant enquiries (see [chapter 6](#));
- The long-term management of data and human tissue, including after the end of the study (see [chapter 8](#));
- The possibility of (re)using the data or the human tissue for future research (see [chapter 9](#)).

1.3 Review, notification and implementation of data protection impact assessment (DPIA)

1.3.1 Submit the [study file](#) to a competent authority and/or to an assessment procedure of the relevant institution(s) and [provider\(s\)](#). Start the study only after receiving a positive assessment from the competent authority and/or institution.

For research that is subject to the WMO (and after the WzI has entered into force, also for research involving human tissue), medical and ethical review by a recognised medical ethics review committee (MEC) is mandatory. In addition, institutions have their own approval procedures. Research institutions, providers and [administrators](#) use different procedures for research that is not subject to the WMO. Data and biobanks usually have an access policy in which a privacy committee or *Data Access Committee* (DAC) plays a role (see [chapters 8](#) and [9](#)).

National initiatives on testing and assessment procedures

Various national initiatives are currently underway to simplify and harmonise testing and assessment procedures. This Code of Conduct is intended to contribute to this process with shared norms and standards. For advice on the assessment of research from a data protection perspective, see [chapter 11](#).

1.3.2 Report the data processing in accordance with the usual procedure to the relevant institutions for inclusion in the register of data-processing operations.

It is important that research, after approval, is recorded in a processing register of the research institution. This is a requirement of the GDPR. Every institution should have a procedure for this. If the researcher is not familiar with this procedure, consult a privacy officer or the DPO.

1.3.3 Check whether the research involves data processing with a high privacy risk. Ensure that for such research a *data protection impact assessment* (DPIA) has been or is being carried out by, or under the responsibility of, the research institution.

Be aware of the fact that much health research may involve a high privacy risk. Legally, the implementation of a DPIA is the responsibility of the [research institution](#). Performing a DPIA can be part of the approval procedure for research in an institution (see norm 1.3.1). Institutions often use their own models and procedures for this. In case of doubt, always ask for advice from the *privacy officers* or DPOs involved.

A DPIA can be omitted if the research institute has already carried out a DPIA on a very similar data processing and the data protection measures from this also apply (almost completely). In this case, ensure that the DPIA, or a reference to it, is added to the documentation of the study. Make it available to interested parties on request.

What is a high privacy risk?

The [European Data Protection Board \(EDPB\)](#) and [the Netherlands Authority for the Protection of Personal Data \(AP\)](#) have formulated criteria and rules of thumb that can help determine whether a privacy risk is high. Translated to health research, this involves a combination of at least two of the following factors:

- *Large scale processing. For example, due to the number of people whose data are processed, the amount and/or variety of data, the duration and/or geographical spread of data processing;*
- *Processing of special category data or data which are regarded as extra sensitive. For example, data from medical files;*
- *Use of new, special or data-intensive techniques. For example, whole genome sequencing or Artificial Intelligence (AI) applications;*
- *Processing of data of vulnerable participants, such as children or patients;*

- *Linking of databases in a way that participants cannot reasonably expect. For example, because the databases have different data controllers;*
- *Research with special consequences for the participant (see [chapter 3](#) and [chapter 4](#)).*

1.4 Responsibilities for institutions

1.4.1 Facilitate the execution of all necessary [DPIAs](#). Also clarify when a DPIA is not necessary because it has already been carried out for this form of health research, or when – as an intermediate form – a 'DPIA light' will suffice, namely when the research requires a variation of an already existing DPIA.

To this end, it is necessary that information is available to researchers on already carried out DPIAs and their scope.

1.4.2 Ensure that after notification by the researcher (norm 1.3.2), the origin, legal [basis](#) and whether or not the [participant](#) has given consent are recorded for each data file. If data are provided to a new data controller, it should be possible to clarify which data were concerned and, of course, to whom they were provided. The same applies as noted above for new data controllers.

These standards should be seen as an elaboration of the register of data processing that every data controller should have. Such a register consists of 'metadata'. The metadata that should be included in the register in the context of data protection in health research have been described above. In addition, the register will also have to describe which categories of data are involved, at least for each processing operation.

1.4.3 Ensure proportionate review and assessment of research

The Code of Conduct prescribes that research should be assessed or reviewed prior to processing (norm 1.3.1), but not how this should be done. Particularly for health research that is not subject to the Medical Research Involving Human Subjects Act (WMO) (nWMO research), there are diverse assessment procedures. The Code of Conduct makes a number of recommendations below on how data protection in such research can be safeguarded through assessment.

- a. Strive for orderly start-up/assessment procedures that integrate different aspects of assessment such as medical ethics review, privacy and data protection, local feasibility and quality assurance, and scientific assessment (a so-called 'one-stop shop');

- b. Assess researchers proportionately. In doing so, take into account the different risks (regarding data protection) involved. Research with limited privacy risks or controlled by a standard approach can, for example, be reviewed by a self-assessment or a quick assessment by an officer appointed for this purpose (a science coordinator, quality coordinator or the secretariat of an ethics committee). Research with a potentially high privacy risk, such as research with [special risks or consequences](#) for the participant, requires a more extensive assessment by an ethics or privacy committee;
- c. Avoid duplication of integral assessment or review in multicentre research. Limit assessment of research that has already been assessed elsewhere for scientific quality and conformity with data protection rules and this Code of Conduct to questions of local suitability and conformity with institutional policy.

2 Appropriate safeguards

For a number of rules and principles, the GDPR leaves more room for [scientific research](#) than for other types of [processing](#), provided that so-called appropriate safeguards are in place. This means that technical and organisational measures must be in place to implement the principle of [data minimisation](#). This chapter describes the measures that must be taken in each case. This also gives substance to the principle of '*data protection by design and default*'.

2.1 Data minimisation

2.1.1 Make sure that only data and [human tissue](#) that are necessary for answering the research question, or for achieving the research purposes, are processed. Take this into account during the entire research process, including processing with other parties.

Which data and human tissue are necessary therefore depends on the research purposes and the methodological foundations in the research or [collection protocol](#) (see [chapter 1](#)).

Take into account the following when designing the data processing:

- Inclusion and exclusion criteria for [participants](#): only include data and/or human tissue from participants to the extent necessary to achieve the aims of the study;
- Selection of data and human tissue: only select data and human tissue that are necessary for achieving the purposes of the study. Document the need for the variables to be used preferably as part of the study protocol or [data management plan](#);
- Data abstraction: process personal data in no more detail than necessary for the purposes of the study, and generalise or group whenever possible. For example, use age categories instead of birth dates or years if that is sufficient to answer the research question;
- Separation of data and human tissue: separate [direct](#) and [indirect](#) identifying personal data as much and as quickly as possible, to the extent possible given the purposes of the research;
- Anonymisation, coding of data and human tissue: Work with anonymised data as much as possible or, if this is not possible, with [coded](#) or pseudonymised data. Only work with directly identifying data if this is necessary (temporarily or otherwise) for the research (see [section 2.4](#)); *and*

- Data erasure: delete data files regularly and promptly that are no longer needed for the research. Think in particular of temporary research files.

If necessary, take additional technical measures when sharing data with third parties to further reduce identification risks, such as adding noise (*obfuscation*) to a dataset.

A good set-up of data processing can be specialised work. If necessary, consult the support services in the organisation.

Collection and processing of data and human tissue without a specific research question

The collection and processing of data and human tissue without specific hypotheses is not excluded from a data protection perspective, as long as it serves a clear purpose. The requirements of data minimisation and, if applicable, as specific consent as possible should be taken into account (section 4.4). A protocol can describe the general purposes of the processing, which phases in the research or data processing can be distinguished, and why specified data, human tissue and data sources are necessary at which phase to achieve the research purposes. Such a phased approach is relevant, for example, in the development of applications using artificial intelligence (AI), data-driven exploratory research, large-scale data registrations, and the special collection or sampling of data and human tissue in a data or biobank for future scientific research.

2.2 Data protection when providing

2.2.1 [Anonymisation](#) and coding should be carried out as much as possible 'at the source', the primary party responsible for processing/providing. This may or may not be done by involving a [Trusted Third Party](#) (TTP).

2.2.2 Provide and process anonymous data only as needed for the research to be carried out with them. If this is not possible, then provide or process coded data. Only provide or process directly identifying data to the extent necessary for the study (see [section 2.4](#)).

2.2.3 Take into account the possible feedback of [findings](#) to the participants. If desired or promised to the participants, the data can be provided pseudonymised rather than [one-way coded](#). In the case of one-way coding, there is no key to return the findings to the participant via the [provider](#).

2.2.4 If data at the level of an individual participant have to be combined from different providers at the [research institution](#), in principle, a TTP should be used for the matching.

2.2.5 When coding, bear in mind that it must be possible to exercise the participant's rights (e.g. to withdraw consent) through the provider. This means that coding that is not carried out via a TTP must

be systematic and reproducible. A self-created list of directly identifying data by code number will not easily meet this requirement.

2.3 Prohibition on reidentification

2.3.1 Researchers are prohibited from tracing coded data back to the directly identifying data of participants, unless the participants have given their express consent.

2.3.2 As a provider, include such a prohibition, where applicable, in the agreement(s) under which data are provided. Also take into account the possibility for participants to withdraw consent or to object (as applicable), if participants can be indirectly identified from the data provided ([sections 4.8, 6.6](#)).

2.4 Processing of directly identifying personal data

2.4.1 Keep communication data separate from research data.

Communication data can be linked to study data via an internal administration number without any content (e.g. a study number). The file with communication data and study number should always be kept separate from the file with the study data.

2.4.2 Only process directly identifying personal data for research purposes to the extent necessary for the research.

Legitimate reasons for processing directly identifying personal data (including communication data) may include:

- The data are necessary for answering the research question (i.e. they are necessarily part of the data set to be analysed);
- To generate a pairing key (code number), if pairing is provided in the protocol;
- To inform participants of individual findings;
- To be able to approach participants during the research for questions directly related to the research purpose, for example for clarification of given answers;
- To maintain contact with participants if that is in the nature of the research (for example, in a long-term cohort study), provided the participant has given consent (see [chapter 3](#));

- To inform participants about the general results of the study, provided the participant has given consent (see [chapter 3](#)); *and/or*
- To contact participants about participation in new or follow-up research, provided the participant has given consent (see [chapter 3](#)).

2.5 Access control

2.5.1 Only researchers and research support staff, such as ICT staff and data managers, who are necessarily involved in the data processing should have access to the data and/or the human tissue. And then only to data that is necessary for the performance of their role in the research.

2.5.2 Make sure or check that the assignment of roles and access rights in the research environment is correct and up to date. Notify the [administrator](#) of changes in a timely manner. Verify this periodically and document the checks.

2.5.3 The processing of research data must take place in an environment that has been assessed by the organisation as being sufficiently secure. This environment must support supervision of the exercise of roles and rights, for example, by the principal investigator.

2.5.4 It is preferable to have a clear separation of functions between those who should have access to the [communication data](#) and those, such as researchers, who should have access to the *research data*. If such a separation of functions cannot be achieved, indicate in the protocol why this is not possible, and why researchers should combine both functions. This may be the case, for example, if the researcher has direct contact with participants.

2.6 Responsibilities for institutions

2.6.1 Align as much as possible with the NEN norms concerning data security in healthcare. Where relevant, apply them accordingly to [data processing](#) in health research.

2.6.2 Provide a role-based access control for researchers that can be properly maintained but also monitored.

Here, the corresponding application of the NEN norms, particularly NEN 7510, is important (see 12.1.2). NEN 7510 has been constructed in accordance with the ISO norm 27001/2. In the context of health research, the latter standard is a fully fledged alternative.

Under certain circumstances, ICT staff must also be able to access the [communication data](#) and research data (as 'super users'). This will need to be set out in a procedure concerning their role and safeguards with regard to confidentiality.

2.6.3 Design this system so that a distinction can be made between those who need access to the communication data (for example, as described in [chapter 4](#), to be able to update participants on developments and/or to invite them again or, for example, to object at a later date) and those who are allowed access to the research data for the intended analyses.

Although NEN 7510 does take into account who has access to what, the distinction between communication data and research data is less pronounced. If there is access in patient care, it is almost always to [directly identifying data](#). In health research, the aforementioned distinction between contact data (which is always directly identifying data) and research data (with as little directly identifying data as possible) is crucial.

2.6.4 Where the Code of Conduct refers to 'coding', this coding can take place internally if the research data are analysed within one research institution, such as an UMC. Such an organisation has often set up a system, together with its ICT supplier, consisting of an EPD with patient data and a research environment derived from it with [coded data](#).

In the example given, provider and researcher are under the same data controller.

2.6.5 If the research data are provided to another data controller, coding via a [TTP](#) is preferable. TTPs have proven methods for generating a non- or hardly identifiable code number. There is also an option that the provider can generate such a secure code number himself.

2.6.6 The Code of Conduct states that, in principle, a TTP must be involved if data concerning a given participant are combined from different providers at a research institution ([section 2.2](#)). In the case of an exemption to this principle, it will be necessary for the data controller(s) to justify why the same guarantees are still achieved with regard to, in particular, the security and reproducibility of the pseudonym among the various providers as without the involvement of a TTP (apply or explain).

2.6.7 A TTP must comply with NEN norm 7524/2019.

Such a switch can guarantee that a secure pseudonym (which can only be traced back to the provider) or a basically unidentifiable code number (which cannot be reasonably identified by anyone) is generated in an identical way everywhere. Which of the two options is most appropriate depends on the circumstances. For an example, see norm 2.2.

2.6.8 The prohibition of reidentification should be reflected in the personnel policy of the research institution and should be facilitated as much as possible by the ICT environment in which the research data are processed.

2.6.9 Prevent researchers from devising and applying alternatives to process [research data](#) outside the safe framework provided by the research institution.

Norm 2.6.8 will have to be worked out in a policy sense, for example in a labour regulation or similar arrangements, as well as in an ICT-technical and facilitative sense. Ideally, it means that the data from the provider can be entered directly into the research database and that only the results of the analyses can be downloaded from it. The research platform must therefore be able to run all relevant statistical software. The less support and fewer opportunities researchers are offered to work in a secure environment, the more they will look for alternatives. However, the research institute will always remain liable to participants and supervisors as the party responsible for processing the data.

3 Informing data subjects

This chapter is about the obligation to provide general information about data processing as it follows from the GDPR. In the case of health research, this consists of two parts:

1. Information on data processing, the privacy statement; *and*
2. Information on the study.

In the first part, the data processing is mainly explained. Providing this information is an independent obligation under the GDPR. It must always be complied with, regardless of the basis of the data processing, even when consent in the sense of the GDPR is not the basis. Both the provider and the research institute (if this is another party) must provide this information. For the research institute there are sometimes exemptions to the obligation to inform each individual participant. These are discussed below.

The second part of the provision of information is intended to enable data subjects to make an informed decision as to whether or not to participate in the study and, if it is prolonged, to continue to participate. This is discussed in more detail in chapters 4 and 5.

The first part (the general privacy statement) is usually not formulated by the researcher but will be part of the organisation's GDPR compliance policy. For the second part, the researcher must provide specific input. The researcher will have to consider whether the general privacy statement includes everything that is important for the potential participants. Privacy statements are often very general. In that case, more should be included in the research information, or the privacy statement should be amended. Concerning providers, it is particularly important that the secondary use for scientific research is explicitly mentioned.

3.1 Informing data subjects about data processing

3.1.1 Under the GDPR, it is compulsory to inform data subjects, both participants and potential participants, of the following:¹⁰

- a. The identity and communication details of the [controller\(s\)](#);
- b. The communication data of the [DPO](#);
- c. The background and purpose of data processing;

¹⁰ We limit ourselves here to the information that is important in the context of scientific research, even though the primary reason for the data processing may not be scientific research but, for example, patient care.

- d. The types of data (and human tissue) that are processed;
- e. The so-called [basis\(s\)](#) or legal basis(s) for processing (see the next two chapters for those bases in research);
- f. If the basis is a legitimate interest (or if one of several bases is, which one is concerned), how has that legitimate interest been fulfilled;
- g. The possible recipients of the personal data (within a healthcare provider, this can also be the researcher if the data has been collected primarily for patient care);
- h. The retention period of the data or, if this is not possible, the criteria used to define that period (see [chapter 8](#));
- i. The possible transfer of personal data to parties in countries outside the EU where the GDPR does not apply, and where no adequate level of protection can be guaranteed;
- j. If the data processing is based on consent: that consent may be withdrawn at any time, without affecting the lawfulness of the processing before the withdrawal;
- k. The rights of the participant (such as access, objection, portability, erasure) with regard to data processing. In the context of scientific research, these rights have been partially clarified (see [chapter 6](#));
- l. The right of the participant to lodge a complaint with the Personal Data Authority; *and*
- m. If the data have been provided by another party (thus not within an organisation such as an UMC where – coded – patient data are provided internally for research): information about the origin of the data, which parties or categories of parties have provided data (see also [section 6.2](#) below).

The Code of Conduct goes on to specifically address information that needs to be stressed about participation in the study. See chapters [4](#) and [5](#).

Points of attention when informing potential or current participants

When providing information on the processing of data and human tissue in research, keep the following points in mind:

- *Give the information in clear, simple language that the participant can understand. Avoid complex sentences, abstractions and ambiguous phrasing. Avoid jargon (legal, technical and specialist terms) except where unavoidable (such as regarding the basis);*
- *Take into account the environment in which the information is provided (digital, physical, telephone). Match the way of providing information to the context of the contact with the participant;*

Preferably offer the information in layers. This prevents information fatigue and makes the information both complete and understandable. The main points must be clear to the participant beforehand. In a digital context, display the first layer of information in such a way that the participant has a clear overview and knows where to find more detailed information.

3.2 Exemptions to the principle of informing by the research institution

3.2.1 The research institution is not required to inform participants personally in the following situations:

- a. If the research is conducted with [coded](#) data provided by other parties, in such a way that participants cannot be uniquely identified in the data (see [section 6.1](#)).
- b. If the research is conducted with data provided by another party, and the participants have already been informed by the provider;
- c. If the research is conducted with data provided by another party and personally informing participants would make the research (the purposes of processing) impossible or seriously jeopardise it. For an assessment framework, see also the exemptions to the principle of GDPR consent (see [section 5.4](#)); and/or
- d. If there is a legal obligation for the data processing, for example for certain types of processing under the Public Health Act.

3.2.2 If participants are not (or cannot be) informed personally, make the information on the study (and data processing therein) publicly available. Make sure that this information is easy to find, for example via your own website or the website and/or the general privacy statement of the [research institute](#). See also [chapter 6](#).

3.2.3 In this case, state which providers (or types of providers, such as ‘your general practitioner’) are providing the data. The provider knows what data have been given to the research institution and should give the participant a copy of this information if he/she so wishes. If participants cannot exercise their rights through the research institution, they can do so through those providers ([section 6.1](#)).

Of course, this information can only be realised at the level of the research institution. The researcher should be aware of this. It will be possible to refer to this in the research protocol.

3.3 Information and control of provision for secondary use: responsibilities of the provider

3.3.1 Ensure that data subjects whose data or human tissue may be disclosed for secondary use are personally informed of this.

3.3.2 Make sure that this information reaches the data subjects with a high degree of certainty so that they can take note of it. This information should also give data subjects the opportunity to exercise control over the provision of data and human tissue for secondary use, and inform them about how they can exercise this control. For more information on this control, see [chapter 5](#).

4 Conditions for research involving the collection of new data and human tissue from participants

This chapter deals with research for which data and [human tissue](#) are collected or taken from [participants](#). This includes research that is subject to the WMO. It also deals with non-WMO questionnaire research, long-term observational research, or the collection of human tissue for management in a biobank for future scientific research.

Such research is often also subject to legislation and international ethical guidelines for medical and health research, in addition to data protection legislation. For example, medical research involving test subjects must meet the requirements of the WMO. And for the special removal of human tissue, the WzI will eventually apply.

Consent for participation in such research is a fixed legal and ethical principle. Consent covers various aspects, including issues such as the physical risks and strain to which participants are exposed. In principle, consent must also be sought for the processing of personal data and human tissue involved in the research. Following on from the previous chapter on information provision obligations, this chapter discusses the conditions consent must meet from a data protection perspective.

4.1 Approaching potential participants

4.1.1 Only approach potential participants about participating if you already legitimately have their communication data.

It is permissible for a researcher to approach people to participate in research if their consent has been obtained previously, for example by participating in previous research (see [section 4.4](#)).

Researchers may, in principle, approach patients with whom they have a treatment relationship as a care provider for participation in research. Think of a physician-investigator who approaches his or her patients. However, it is preferable that a participant is asked for consent by someone with whom they have no dependency relationship ([section 4.7](#)). An involved care provider should always weigh up whether it is appropriate to invite a patient themselves. The admissibility of this in a specific case is also assessed by a medical ethics review committee in research that is subject to the WMO.

4.1.2 Under certain conditions, it is possible to approach potential participants using communication data provided by a provider.

Under the following circumstances it is possible for researchers to lawfully receive communication data:

- a. The Rijksdienst voor Identiteitsgegevens (RvIG) makes a selection of communication data from the Personal Records Database (BRP) requested by the researcher and provides this to a research institution. This is subject to a separate authorisation procedure under the BRP Act;
- b. The party that holds the communication data – for example, a care provider or market research company – has the consent of the [data subjects](#) to provide communication data to the researcher; *or*
- c. The party that has the communication data at its disposal provides them to researchers on a different basis, without the consent or objection of those involved. This is only possible if it concerns data from which no characteristics about illness or health can be derived and if the privacy statement states that certain personal data will be provided to a third party. Approaching patients or clients for participation in research is only possible in one of the other ways discussed here.

4.1.3 It is permissible, under certain conditions, to approach potential participants through another party that is in contact with them and who approaches them on behalf of the researchers, without providing communication details directly to the researchers.

This method is ideally suited for approaching potential participants from a healthcare setting (in contrast to norm 4.1.2.c), if the healthcare provider itself is not involved in the implementation of the study. Local procedures should be taken into account. For example, some [healthcare providers](#) record whether patients have objected to being approached for research. Approaching participants via a market research agency can also fall under this.

Approaching potential participants via another party: an example

Often a healthcare provider will invite patients or clients for research initiated by a [research institution](#). In this example, the healthcare provider is not also the research institute where the research will be conducted. The invitation contains general information about the study. Patients who are interested can contact the researchers, for example via a link to a website or a reply form, and thus start the consent procedure.

Researchers should not have the communication data of these patients or clients at their disposal before starting the consent procedure. At the same time, the healthcare provider does not need to know which patients or clients have responded. To guarantee this, the healthcare provider can also make use of a [processor](#), for example a 'mailhouse'. This processor can send out the invitation, keep track of the response and send reminders if necessary.

4.1.4 It is permitted to approach participants through or by means of a recruitment campaign. However, recruitment via social media requires special attention from a data protection perspective.

Invitations or advertisements for research on social media are complex from a data protection perspective for several reasons. Most social media platforms often process data outside the European Union (EU), which can be legally problematic. In addition, platforms may themselves unlawfully infer characteristics about the illness or health of interested parties from invitations or advertisements for health research. The use of characteristics directly related to a certain disease to determine the target group of advertisements is therefore problematic. General characteristics such as age, gender or interest in sports are generally not a problem. Seek expert advice on this, for example from a privacy officer or possibly the DPO.

4.2 Explicit prior consent to data processing

4.2.1 Ask participants explicitly to consent to the processing of their data and human tissue prior to the collection and processing for research purposes.

Distinguish consent for data processing from consent for other aspects that may be involved in research, and from consent for other matters, such as data exchange in the context of treatment. Consent for data processing cannot be 'inferred' from consent to participate in research.

Simply asking consent to participate in research is therefore not enough. It must also be accompanied by clear, separate information on and consent for data processing. This is in line with what is stated in [chapter 3](#) about the provision of information. Because the research institution now obtains the data directly from the potential or current participant, participants should be informed about this personally. Any exemptions to this ([section 3.2](#)) do not apply.

Consent for data processing must also:

- a. Be informed (see norm 4.2);
- b. Be specifically granted (see norm 4.3);
- c. Be further specified in case of long-term, wide-ranging research (see norm 4.5);

- d. Be given freely (see norm 4.6);
- e. Be demonstrably given (see norm 4.7); *and*
- f. Be as easy to withdraw as it is to grant (see norm 4.8).

These conditions are elaborated on below. In order to distinguish them from other forms of consent (see in particular [chapter 5](#)), consent that meets these conditions will be referred to below as *GDPR consent*.

Data processing in clinical trials of medicinal products: legally not GDPR consent

Separate legal conditions apply to data processing in the context of clinical research into medicines. Participants do give their consent to participate and also receive the privacy statement discussed in the previous chapter. However, this informed consent for participation in the clinical study of medicinal products is not GDPR consent. The informed consent leads to compulsory data processing with regard to the safety and efficacy of the medicinal product and the reliability of the conduct of the [trial protocol](#). This processing is thus based on a legal obligation.

However, the participant must be informed of what such data processing entails (see [section 5.3](#)).

For research outside the research protocol with the data collected in this way, separate GDPR consent must be obtained in accordance with the conditions elaborated in this Code of Conduct, as for other research (see also [section 6.5](#)).

4.2.2 Take into account separate rules on representation by a legal representative when asking for consent in research involving minors under the age of 16 and incapacitated participants.

Under the UAVG, minors under 16 years of age cannot themselves consent to the processing of data relating to them.¹¹ They are represented by their legal representative, i.e. parent(s) with parental authority or their guardian. Consent for participation in the study must therefore be requested from these representative(s), even if the data is collected from the minors themselves.¹²

The UAVG also states that people who have been placed under guardianship or mentorship or who are under administration cannot give their consent. However, the qualification is added that this only applies to matters for which the person in question is incompetent or unauthorised. This cannot be

¹¹ There is an exemption to this for help and advice services that are offered directly and free of charge to a minor or a person under guardianship. Think of the child helpline.

¹² It has already been noted in the introduction that this may limit certain health research, such as observational research into domestic violence, where the voice of the child or young person would actually be heard. This dilemma and any specific standards for this type of research are not addressed in this Code of Conduct.

assumed for participation in a questionnaire study. For participation in research that is subject to the WMO, this must be assumed for persons placed under guardianship or mentorship. If in doubt, consult a legal expert or the MEC.

Furthermore, it is important to take the following into account:

- In accordance with the system of the Wgbo, children from the age of 12, provided they are legally competent, have an independent right to confidentiality of patient information. If consent to withdraw information from the child's file is also requested, the child from the age of 12 must consent. This also affects chapter 5. The GDPR consent that is described there concerns double consent: both the consent of the children in the 12-16 years old group and that of their legal representatives. The objection system would involve the objection of the group of 12-16 year olds.
- The WMO also has a condition for double consent for the group between 12 and 16 years of age and special provisions concerning what research may be carried out with which group of people under 16 years of age or those who are unable to give informed consent. These special conditions are not specific to data protection and fall outside the scope of the Code of Conduct.

Research in emergency situations

The CCMO has drawn up a step-by-step plan for delayed consent in research that is subject to the WMO in emergency situations. This step-by-step plan requires that the [trial subject](#) or his legal representative(s) be asked for consent to participate (or continue participation) promptly, as soon as the situation allows. Asking consent for data processing in the framework of the study is part of this. For exemptions to consent for secondary use of data and human tissue in emergency situations, see [section 5.4](#). Dealing with delayed consent and representation in non-WMO research could not be dealt with in the scope of this Code of Conduct. It is expected that outside of WMO situations, the direct collection of data from participants will not occur, or will occur only extremely rarely. In these situations the potential participants will also not be able to provide the data.

4.3 Informed consent

4.3.1 Fully inform participants about all aspects of data processing that are essential for making a choice about participation and data processing.

4.3.2 Participant information on a specific study may refer to general information on data processing of the institution, such as a 'privacy statement' (see previous section). In that case, make sure that participants are familiar (capable of being familiar) with this information. When giving consent, they should declare that they have done so.

4.3.3 Provide the information to the participant before asking consent.

Make sure that the participant information covers at least the following topics, as applicable:

- The information mentioned in [chapter 3](#);
- The background and purposes of the study;
- The duration of the research and data processing, including the retention period;
- The efforts expected of the participant in the study;
- The types of data and human tissue processed for the study;
- The types of parties that may be involved in the study and/or to whom data will be disclosed (e.g. whether commercial partners are also involved and their role in the study);
- The [special consequences](#) that the processing (or parts of the processing) of data or human tissue may have for the participant (see [section 4.4](#));
- Other aspects or parts of the study about which participants should be separately informed and/or for which they should give separate consent (see [section 4.4](#));
- The likelihood of individual [findings](#) and how they are dealt with (see [section 4.4](#)); *and*
- The possibility for the participant to withdraw consent at any time (see [section 4.8](#)).

This information can be bundled in one brochure, for example a participant or trial subject information brochure in WMO terms. It is also possible that the participant information refers to a separate privacy statement of the institution involved (see [chapter 3](#)). In that case, make sure that this privacy statement is easily accessible and be as clear as possible about the way in which data are processed.

4.4 Specific authorisation

4.4.1 Ask participants to consent to the processing of data and human tissue as specifically as possible, given the purposes of the research or collection to be undertaken.

Base the purposes for which consent is sought on the research or [study protocol](#). This specifies and substantiates the purposes and research questions. If the protocol does not include a specific purpose, make sure that the purposes are at least delineated by a particular field of research that is recognisable to participants. This could be research into a particular clinical picture and related disorders, into healthy ageing, or into the influence of the environment on public health.

4.4.2 Distinguish clearly between processing operations or parts of the research that are necessary for the achievement of the main purposes and those that are not. Obtain separate consent for the latter, via a separate consent or *opt-in* request. Unless the research cannot otherwise be carried out at all (in other words, this link is inherent to the research as described in the research protocol), this applies to linking research data with other data sources. Of course, this linking must be mentioned in the information. In addition, this also applies to the possibility of use, re-use or issue in future research and to the processing of communication data (see [section 4.4](#)).

Separate consent refers to consent for a specific purpose or part of data processing, via an opt-in that participants can grant or refuse separately. This opt-in can consist of boxes which the participant can tick with a yes or a no.

4.4.3 Inform participants about any special privacy risks or consequences that the research (processing of data or human tissue) or certain applications in it may have. Ask consent for such applications and research separately. Make such consent part of a broader consent request only if this is necessary to achieve the main purpose of the research, and the participant explicitly consents to the special risks or consequences.

Research can have special privacy risks or consequences for the participant in various ways. It can also involve a high privacy risk. It may involve research or applications with possible personal consequences for the participant, such as for his or her treatment. It may also involve processing that could jeopardise the privacy or rights of participants. And it may involve research or applications that can be considered sensitive for society or the participant and/or have been designated as sensitive in legislation and regulations. Processing and applications to which this applies are:

- Research and applications with a significant risk of individual findings (see [section 6.8](#));
- Research with data that is considered intrinsically identifiable, for example whole genome sequencing, and where this data is shared more widely than within the research institution where the sequencing takes place;
- Transfer of data to parties in countries outside the EU where the GDPR does not apply and an adequate level of protection cannot be guaranteed;
- Purely commercial research where the results are made available exclusively to a private, profit-oriented party;
- The amplification of human tissue into immortal (stem) cells and cell lines;
- The amplification of human tissue into germ cells and embryo-like structures;

- Human-animal combinations in which there is a substantial admixture of genetic material of human and animal origin (e.g. cybrids and chimeras).

Research with genetic data does not necessarily have special risks or consequences for participants. Think of research where the chance of individual findings is minimal and where data is not considered intrinsically identifiable, for example because it is limited to part of the genome or certain genetic variants.

4.4.4 Inform participants of the intended data links in the context of the study. In principle, ask consent separately. Only make this consent part of an overall consent request if this is necessary to achieve the main purposes of the study, and the participant explicitly consents to the linking of his or her data.

It is important that participants are informed about the types of data used, types of purposes for which links are made, and types of data sources between which links are made. Consent does not have to be given separately for each source to be linked. For example, information about the various data sources can be offered in layers. The first layer, which the participant always sees, states in general the types of data sources. Then, in more extensive background information, an overview can be offered of all the sources and data controllers to which data are linked.

Links with the causes of death registration of the Central Bureau of Statistics (CBS) are subject to a separate legal regulation. Participants must therefore be informed separately about this link and grant separate consent. For more information and a sample text, see [CBS](#).

4.4.5 Inform participants about the possibility of (re)using data and supplying human tissue for future research. Ask consent for this separately. This consent can follow a broad consent request if this is necessary to achieve the main purpose of the research and the participant explicitly grants consent for such future research.

Ensure that participants are adequately informed of the purposes and conditions under which future research will be conducted. Information about this can be brief if the future processing fits within the primary purposes and conditions of the study.

Always ask for separate consent if this collection and processing are primarily aimed at a specific research question, such as in the case of research that is subject to the WMO. Possible re-use must be justified in the research protocol and must fit within the purposes and conditions of the original research. See also chapters [1](#) and [9](#).

4.4.6 Ask participants separately for consent to process communication data after the end of the study.

Consent can also be considered as given by the fact that the participant has left communication data behind on request. Reasons for storing communication data longer include the possibility of sharing research results and inviting participants to participate in follow-up research (see [section 2.4](#)).

4.5 Further specification of consent in the case of wide-ranging research

4.5.1 If, at the outset, the purposes of research and the processing of data and human tissue cannot be fully defined and participants are thus asked to consent to broad purposes, ensure that consent is further specified by other means prior to and/or during the research.

4.5.2 Inform participants in an appropriate way about the research activities carried out with their data and human tissue within the broad purposes. What is appropriate depends on the context in which data and human tissue are collected and participants' expectations of such information. Where possible, make additional information about the sub-studies available, such as a study plan or protocol. In any case, make information about the course of the study and any results available and retrievable.

4.5.3 Ask consent again for a sub-study if it involves particular privacy risks or consequences, and participants have not previously given consent for such a study (see [section 4.4](#)).

4.5.4 In other cases, offer participants additional ways to exercise control over their data and human tissue, where appropriate and feasible. Think of digital environments for managing consent, and specific opt-ins and opt-outs.

4.5.5 Provide a control mechanism to ensure that research is consistent with the consent previously granted by participants. For example, by setting up a *Data Access Committee*.

The standards in this section are relevant to long-term, broad-based research. The purposes of such research are often formulated in general terms. Think of the establishment of a biobank for a certain type of

disease. Or longitudinal research on the neurocognitive development of children, or the healthier ageing of people.

In principle, these standards are not relevant to research that is subject to the WMO. The purposes of the processing of data and human tissue for such research are specifically described in the research protocol, and the information for test subjects is geared to this (see chapter [1](#)). Participants (test

subjects) must be able to grant separate consent for the re-use of data and human tissue. Such re-use must be in line with the purposes and conditions of the original study (see [section 4.4](#)).

Consent which cannot be given in a fully specific manner at the outset, due to the broad purpose of the research, must still be sufficiently specified in other ways. The appropriate form depends on the circumstances and specific situation of the research. Firstly, it is important that the purposes or fields of research are and remain delineated. Secondly, the sub-study must remain clearly linked to the context in which the data or human tissue was collected. Finally, the expectations of participants must be taken into account. It is neither necessary nor desirable for participants to be able to give their consent for each sub-study separately.

Communicating with and involving participants in the organisation of research are important aspects in this regard. This can also help in choosing and substantiating an appropriate form of information and specifying consent. It is therefore advisable to involve participants as allies in the research. Consider special forums, physical meetings, videos with explanations, Q&A forums, participant panels and sounding board groups, and representation on advisory boards.

4.6 Freely granted consent

4.6.1 Ensure that participants can freely give and withdraw consent.

For consent to be freely given, potential participants should not be disadvantaged by its refusal or withdrawal. Participants must be free to choose whether or not to give consent.

In research in which patients participate, make sure, if possible, that the patient is not in a relationship of dependency with the person requesting consent. A decision on participation and processing should not have any consequences for the treatment, whatever decision the patient makes. The participant information should clearly state this.

In the information and consent procedure, pay attention to possible misconceptions about the supposed benefits of participating in research (the so-called therapeutic misconception). Ensure that this misconception is avoided as far as possible.

4.7 Demonstrable consent

4.7.1 Make sure that it can be demonstrated that consent was given, and how.

For research that is subject to the WMO, the general requirements for consent to participate in such research can be followed. This usually requires a written signature. An amendment to the WMO Act that would make electronic consent possible was enacted in 2022.

For research not subject to the WMO, ticking one or more boxes digitally or granting consent verbally can also count as demonstrable consent. However, a number of conditions must be met:

- a. Provide reliable authentication of the participant's identity, especially if consent is given verbally or online (note: authentication is not required for the one-off completion of a questionnaire);
- b. Document the consent procedure, the information participants received and the opportunities (reminder) they were offered;
- c. Ensure reliable registration of responses; *and*
- d. In the case of oral consent: ensure that there is a protocol in place to guarantee that participants have been fully informed, and that consent is only recorded if it has indeed been given. If, in exceptional situations, consent is sought by telephone, making recordings of the conversation can be part of the protocol.

4.8 Withdrawal of consent

4.8.1 The participant always has the right to withdraw his/her consent for the processing (or parts of it) of data or human tissue.

4.8.2 Make withdrawing consent as easy as giving it.

4.8.3 Inform participants clearly in advance about the consequences of withdrawing consent.

Make a clear distinction for participants between ending participation (for example, withdrawing consent to be approached for further participation and new data collection) and withdrawing consent to process data that has already been collected. When only stopping participation, data and human tissue already collected may still be used for research. Stopping will often also be implicit, namely because the participant no longer responds.

If a participant withdraws his or her consent for the processing of already collected data (parts of it), already collected data and human tissue must be deleted or destroyed, unless:

- a. data or human tissue must be retained for replication or validation of previous research results, after the results have been published, or a paper on the research has been submitted for publication;
- b. there is another reason and a legal basis for retention, such as a legal obligation; *and/or*
- c. there are other compelling reasons why this erasure threatens to render the research impossible or seriously jeopardise it. This requires a concrete, specific substantiation. Consider, for example, a substantial risk of distortion of the results which cannot be corrected and which would make the results of the study unreliable.

In such a case, inform the participants concerned of the reason for continuing to process the data or the human tissue.

Consent and the right to erasure of data in clinical trials

For research into medicinal products, there is a legal obligation to process data relating to their safety and reliability under the Clinical Trials Regulation (ECTR). In particular, this concerns archiving of the clinical trial master file, the medical data of participants, and any processing of data in the context of access. The right to erasure does not apply to such data.

5 Conditions for secondary use

This chapter deals with the conditions that specifically apply to the [processing](#) of data and [human tissue](#) in health research that was previously collected for a different purpose. This is known as (a type of) [secondary use](#).

Such research often involves secondary use of [special category data](#) and human tissue that has been collected in the context of individual patient healthcare. As explained in the guide and in the [chapter on controllership](#), the Code of Conduct assumes a division of roles between [providers](#) on the one hand and [researchers and research institutions](#) on the other. In a healthcare context the provider is therefore a healthcare [provider](#) that collects and manages data and human tissue for purposes other than [scientific research](#). This chapter deals with the conditions for both the provider and the researcher or research institution.

The standards below provide a system of guarantees that ensure that [data subjects](#) are clearly informed and can exercise control (and can continue to do so) over secondary use of special category (particularly medical) data and human tissue. The starting point is that [participants](#) are asked for GDPR consent for provision and secondary use. Exemptions to this principle are possible under certain conditions. Which form of consent must and can be requested, and whether an exemption applies, are discussed below. A careful assessment must be made for each research project for which personal data and human tissue are processed. Is this possible under the conditions of previously requested consent for secondary use? Or should and can consent still be requested? Or does an exemption apply (and if so, which one)?

Less strict conditions generally apply to the provision and secondary use of non-special category data. However, this only applies to data that do not contain information about illness and health, not even in derived form (for example, because they have been provided by a healthcare institution). An example is data managed by employers or a pension fund. The rules in this chapter do not fully apply to these situations. In that case, the same considerations must be made as discussed in section 6.2.2 under c. This concerns, for example, the provision of data about the nature of the employment, such as night shifts.

For the record: the (re)use for future research of data and human tissue that has already been made available for research is subject in the first place to the conditions in [chapter 9](#). That chapter also explains how and when the conditions for secondary use apply to that situation.

5.1 Provision and secondary use of anonymous or anonymised data and human tissue

5.1.1 Anonymous or [anonymised](#) data may be provided and processed for secondary use in health research. Providers do not need to ask the data subjects' consent or give them the opportunity to object.¹³ The standards discussed in the remainder of this chapter do not apply in this case. For research with anonymised data, the usual scientific integrity standards do apply, naturally.

5.1.2 Provision of anonymous or anonymised human tissue (usually this is collected in the context of healthcare) is allowed for the time being, unless data subjects have objected to it. Providers must inform data subjects about this and enable them to raise an objection in an easily accessible way ([section 5.6](#)).

Please note: after the WzI comes into force, the standards below (section 5.2 and beyond) apply to the provision of each piece of human tissue. Objecting to or withdrawing consent is no longer possible after human tissue has been anonymised.

5.2 Conditions for secondary use of special category data: consent as the starting point

5.2.1 Check whether consent for secondary use has been obtained from the provider(s) and whether the study fits within the conditions set for it. In the case of secondary use, such consent may be requested by the provider. For the researcher's approach to potential participants and the requesting and granting of consent for secondary use, the conditions as described in [chapter 4 \(section 4.1\)](#) apply.

5.2.2 The consent must, in principle, be GDPR consent. Unless it concerns research with [special risks or consequences](#) for the participant, this can also be general consent in the case of certain healthcare providers, see further on in this chapter ([section 5.3](#)).

¹³ This would be different if the healthcare provider were to issue a more far-reaching statement to patients, for example that, subject to a legal obligation to provide data, the patient will always be asked for consent or can object to secondary use for scientific research, regardless of the nature of the data.

5.2.3 If consent has not been obtained, try to request and obtain consent for the specific study and the provision of data and human tissue for that study (unless this is not possible or cannot reasonably be required). In the case of secondary use, this consent can be requested by the provider.

5.2.4 If consent has not been sought previously and cannot be sought subsequently, ascertain whether one or more exemptions to the presumption of consent apply (see [section 5.4](#)). Substantiate the use of these exemptions for each provider separately.

5.3 General consent for healthcare providers

5.3.1 It is acceptable for healthcare providers who regularly disclose patient data and/or provide human tissue for various health research purposes to ask the parties involved for their [general consent](#) to disclose them and provide them for secondary use. Research carried out on this basis must meet the same conditions as research carried out on the basis of an exemption to the principle of consent ([section 5.5](#)).

5.3.2 For research with [special risks or consequences](#) for the participant, general consent is not sufficient. For this, GDPR consent must always be requested (see [section 4.2](#)).

5.3.3 Make sure that data subjects have been personally informed about secondary use and the conditions under which this will be carried out when asking for general consent ([chapter 3](#)). Give data subjects time to reflect, and bring the request to the attention of data subjects who have not responded.

5.3.4 Inform those involved explicitly that if they do not respond after the request has been brought to their attention again, their data and/or human tissue may be used for secondary use. Also state that in the absence of a response, it will be assumed that they do not object and that they can object at a later date if they so wish. Data and human tissue can be supplied for secondary use if the parties concerned have not made a choice after at least one effective reminder, linked to an accessible opportunity to respond.

5.3.5 Make sure that the general consent can be given and withdrawn in a simple and accessible manner. Also make sure that it is easy to lodge an objection later on.

5.3.6 Before supplying data or human tissue under general consent for each individual study, assess whether it complies with the conditions applicable to it ([section 5.5](#)).

The Code of Conduct does not set any further requirements on the way in which general consent is requested from the parties involved. This can be done verbally, for example, or through a digital system such as a patient portal. Whether this consent is demonstrably given can be demonstrated by, for

example, following a protocol that deals with informing and requesting consent from data subjects and the registration of giving or refusing consent, or noting that the data subject did not want to take a decision at that moment (see also [section 4.7](#)).

In the case of contact with patients who are being treated or with whom contact is maintained, general consent may still be requested at a suitable time. For other patients, GDPR consent must still be requested per study if the healthcare provider wishes to provide personal details to a research institution, unless this is not possible or cannot reasonably be required (see below at [section 5.4](#)). If, prior to the introduction of general consent, the healthcare provider assumed an objection system based on the arguments described in the next section, the coded data of patients with whom there is no longer active contact can be provided on the basis of that system. Exemptions to the principle of consent also remain important for healthcare providers who ask patients for general consent to disclose data for secondary use. Under certain conditions, research with data and human tissue of those involved will therefore remain possible without asking them for consent, or without consent being granted (because they did not respond). (See also [section 5.4](#).)

Different situations are possible:

- a. If data subjects give their general consent, their data and human tissue may be provided and processed for secondary use. This is the case unless and until the data subjects refuse consent or object.
- b. If data subjects have not responded to the request for general consent, their data and human tissue may be provided and processed for secondary use (after an explicit reminder). This is the case unless and until the data subjects refuse consent or object.
- c. If data subjects refuse or object to general consent, their data and human tissue cannot be provided for secondary use.
- d. If data subjects have not been asked for general consent, their data and human tissue may be provided for secondary use on the condition that consent is granted after all, or an exemption to the principle of consent applies ([section 5.4](#)) and a system of objections to secondary use had not already been introduced. Both conditions apply to data or human tissue collected before the healthcare provider started to ask for general consent and to data or human tissue from patients (patient groups) that were not (or could not be) reached when general consent was requested.

Conditions of general consent

With these standards, the Code of Conduct outlines a framework of conditions that general consent must meet if a healthcare institution introduces it.

The position of registries that strive for national, complete coverage (such as the Dutch Cancer Registry) requires attention. Currently, such registries generally operate on the basis of an exemption to the principle of consent (section 7.4). The continuity of such registries must be guaranteed. One direction that can be considered within the current legal frameworks is the development of a more granular system of objection and general consent.

Healthcare providers remain obliged to inform patients individually about the provision of such registrations. They must also offer a low-threshold possibility of objection. This also applies to healthcare providers that do provide regular information, but cannot organise general consent (sections 5.4 and 5.7). The other rules of the Code of Conduct also apply to research with these data and human tissue, such as the need to request specific consent for research with special privacy risks or consequences (norm 5.3.2).

5.4 Exemptions to the principle of consent for special category data

Whether an exemption is justified or not requires a reasoned assessment for each study. This consideration may be different for each provider. The decision to supply data or human tissue based on an exemption is ultimately up to the supplier. Of the criteria listed below, some apply to each individual provider and others (in particular, norm 5.4.2 under b and c) to the study as a whole. The provider is expected to set up assessment procedures for this purpose ([section 5.7](#)). It is recommended that providers make this assessment in a similar way and evaluate or assess research proportionally. For the criteria that apply to the study as a whole, the initial assessment should weigh heavily.

5.4.1 In a number of situations, it is not possible to request consent for a specific study, and the provider has not requested or been able to obtain general authorisation for secondary use ([section 5.3](#)). Whether such a situation applies must be determined for each specific study and for each individual provider.

The circumstances under which asking consent is not reasonably possible are listed below. If possible and reasonable, make a distinction between groups of data subjects to whom the exemption applies and data subjects who can be asked for consent.

- a. *Participants have died.* This appeal is possible if it can be reasonably assumed that a large number of participants have died, based on information about the patients involved or, if this is unknown, based on the average expected survival time. The situation must be prevented that participants who have died are approached and next of kin are confronted with this. The criterion of 'a large

number of participants' can be interpreted both relatively and absolutely. As a rule of thumb, this is the case if more than 50 percent of the participants are expected to have died, but if the research data or human tissue of a large group of participants is required, as a result of which many more relatives would be confronted with the question, this percentage may be lower (see Norm 5.4.2 a).

- b. Current communication data is unknown or probably no longer correct, and there is no possibility to update it. Recourse to this is possible on the basis of a well-founded consideration of the importance of the research, the importance of asking consent, and the risk of data breaches due to e-mails or letters arriving at the wrong address.
- c. *Data and human tissue are collected in emergency situations.* An appeal is possible if data and human tissue have been or will be collected in emergency situations. In emergency situations it is not always possible to ask consent in advance or to offer the option of objecting. Unless the patient is already known to the care provider with a consent or objection system, the patient must still be given the opportunity to give consent or make an objection. If in such a situation the patient has died or cannot be reached, the data can be provided if this is described in the protocol and the provider (or the assessing body, such as an assessment committee at the provider's) has agreed to this exemption.
- d. A combination of the above factors.

5.4.2 In a number of situations, seeking consent cannot reasonably be required, involves a disproportionate effort for the specific study, and the provider has also not requested general consent for secondary use ([section 5.3](#)). Whether such a situation applies must be determined for each specific study and for each individual provider.

The following are the circumstances in which asking consent cannot reasonably be required or requires an unreasonable effort.

- a. *Because of the size, approaching the group of participants requires an unreasonable effort ('large numbers').* This is possible on the basis of a well-founded assessment of the effort required from all parties involved (researchers, healthcare workers, etc.), the availability of low-threshold possibilities to contact potential participants, and the risk that a sufficient response is not achieved within a reasonable time frame and cost. An absolute threshold for the size cannot be given. It depends on several factors, such as the possibility of digital contact with participants. In some situations, contacting more than one hundred patients may be 'disproportionate', in other situations it may be five thousand.

- b. There is a substantial risk of uncorrectable bias in the results, which would make the results of the study unreliable (selection bias or 'consent bias'). Appeal to this is exceptionally possible on the basis of sound methodological and statistical substantiation. This must include considerations and/or evidence of the risks of bias in the results (due to problems of reliability, internal and external validity, for example). It must also be substantiated why there is no possibility of correcting this adequately.
- c. There is a good chance that approaching participants to ask for their consent would place too great a burden on them. An appeal to this is possible on the basis of considerations and/or evidence from scientific (including medical-ethical and psychological) research, professional experience and/or the opinions of lay experts. Consult on this with lay experts or an organisation that represents participants, such as a patient organisation.
- d. There is a risk that people in the immediate environment of the potential participant will see the invitation, in circumstances where it must be ensured that the invitation only reaches the potential participant. An appeal to this is possible based on a well-founded consideration of the importance of the research, the importance of asking consent and the risk that the invitation can be read by people other than the person involved. Think, for example, of situations such as Veilig Thuis (Safe at Home) or a shelter or safe house, where it is essential that invitations for participation reach the previous victim and not, for example, the partner.
- e. A combination of the above factors.

5.5 Conditions of secondary use on the basis of general consent or an exemption to the principle of consent

5.5.1 Research with data or human tissue provided and used on the basis of general consent ([section 5.3](#)), or an exemption to the principle of consent ([section 5.4](#)), must meet a number of additional conditions.

In these cases, GDPR consent is not the basis for processing. Unless the research is based on a specific legal basis¹⁴, such research is subject to a number of additional conditions:

- a. The research must be related to the area(s) of the patient's illness or request for help;
- b. The research serves a general interest;

¹⁴ In a number of situations, this applies to the RIVM. See the legal section.

- c. The research must not have any [special risks or consequences](#) for the participant. Separate (GDPR) consent must be sought for this (see [section 4.4](#));
- d. The study cannot be carried out without these data; *and*
- e. The data or the human tissue shall be provided to the researcher in coded form, or the study may only be performed with coded data or human tissue.

5.6 Provider responsibilities: control of provision for secondary use

5.6.1 Offer data subjects the opportunity to exercise control over the provision of data and human tissue for secondary use. Inform them about how they can exercise this control.

5.6.2 Integrate the provision of information and the opportunity to exercise control as much as possible into the administrative and care routines or work processes of the institution. Dovetail with other ways in which the institution communicates with patients, including the general privacy statement and digital patient portals.

5.6.3 If there is still contact with the data subjects, regularly and appropriately inform them that they have given their consent and that they can object to secondary use.

5.6.4 Offer data subjects a low-threshold possibility of refusing or withdrawing consent, or of objecting to secondary use. Make sure these withdrawals or objections are respected.

5.6.5 Make a note in the medical file of any objections made and consent (general or otherwise) refused or withdrawn, if it concerns disclosure of data collected in the context of treatment.

5.6.6 Make a note in the medical file of any data or human tissue disclosed for the purpose of scientific research.

Depending on the study and the way control is organised, control may consist of:

- a. Providing an option to give GDPR consent for specific research (see [chapter4](#));
- b. Providing a possibility to give general consent for secondary use, if the provider has organised this (see [section 5.3](#));
- c. Providing an opportunity to object to secondary use for research for which an exemption to the principle of consent applies (see [section 5.4](#)); *and/or*
- d. Combinations of these.

Pay attention to secondary use, for example, in the institution's privacy statement (see also [section 3.3](#)). If applicable, refer to specific information about consent or possibilities of objection to secondary

use. Explain that giving or refusing consent and making an objection have no consequences for the treatment, and that patients can also decide later. Address how the institution monitors and assesses whether provision for research is appropriate (for example, the role of a review committee). Provide ongoing, easy-to-find general information about the research in which the institution/provider is collaborating. This can be done, for example, through a separate website on the institution's research, to which the information for those involved refers.

If a provider does not inform data subjects about secondary use and the possibility of objecting to this, this must still be done prior to disclosure. In principle, consent must be requested for such a disclosure. In some situations, however, this is not possible or cannot be required, and it would mean a disproportionate effort for the research (see [section 5.4](#)). In such cases, the above can be met by adequately informing those involved and offering them the opportunity to object. If possible, this can be done by writing to patients personally and offering them the option to object. Otherwise, a targeted advertisement or campaign may be considered. This is not necessary for healthcare providers who have already adequately informed patients about secondary use and the possibility to object.

5.7 Provider responsibilities: institutional policy on secondary use

5.7.1 Establish policies for accessing and providing data for secondary use, with clear application and review procedures that monitor the conditions.

5.7.1.1 Access to data or human tissue for the purpose of provision (at the providing party's premises) without the consent of data subjects is permitted only to or under the direct responsibility of those who already have access to it by virtue of their role in the original purposes of processing.

For access to medical records, this role should be interpreted strictly. Access must be limited to healthcare professionals who have or had a treatment relationship with the patient or staff working under their direct responsibility (including the ICT department). It relates only to those parts of the medical record that are relevant to the part of the treatment in which they were involved. This access can be used for anonymising data or human tissue (see [section 5.1](#)) or for selecting patients to be invited to participate in research (see [section 4.1](#)).

5.7.2 In order to select patients for participation, providers may draw a sample from their files, together with researchers, provided that: data subjects have not objected to the processing of their data for health research purposes; the researcher's involvement in the sample is necessary for

methodological reasons; and access to directly identifying data by the researcher is limited as much as possible in terms of time and amount of data.

In such a case, the research is still in a preliminary phase. The person authorised to do so makes a selection of patients or other data subjects at the request of the researcher. It is important that technical and organisational measures are taken to limit the researcher's access to directly identifying data as much as possible (see [chapter 2](#)).

5.7.3 Ensure that data subjects are initially contacted by people who, by virtue of their role, already have access to the necessary data, or by people under their direct responsibility.

5.7.4 Only provide data from data subjects/patients if it is allowed. Depending on the conditions of the study, and whether general consent has been organised, disclosure can be on the basis of general or GDPR consent, or if data subjects/patients have not objected.

5.7.5 Check as part of the assessment procedures:

- a. Whether research can be done with anonymous data (see [section 5.1](#)); if not:
- b. Whether research can be conducted within the framework of any previously requested consent (GDPR or general) (see [section 4.4](#) on specific consent, [section 5.3](#) on general consent); if not:
- c. If general consent for secondary use or GDPR consent for specific research is still requested, whether the conditions for this are met (see [section 5.3](#) on general consent and [section 4 on GDPR consent](#)); if not:
- d. Whether one or more exemptions to the principle of consent apply to the provision. And if so, whether a reliance on this is sufficiently substantiated (see [section 5.4](#)).

It is recommended that providers test or assess this consideration proportionally and uniformly, as far as possible. With regard to the criteria applicable to the study as a whole, the initial assessment should weigh heavily in this respect.

5.7.6 Ensure that data and human tissue are always provided to researchers [in coded form](#). If personal data have been supplied for research purposes, withdrawal of consent or subsequent objection should be communicated to the research institution(s) under the code number. The research institution should give each provider a secure but simple means of passing on this additional information.

5.7.7 Lay down agreements about the transfer of personal data or human tissue to another organisation in an agreement (for example, a Data-Sharing Agreement or a Materials and Associated Data Transfer Agreement). It is recommended that this also be done when anonymised data are provided.

5.7.8 Include safeguards in the agreement for the careful handling of data protection and (where applicable) compliance with the rules of this Code of Conduct.

In exceptional cases, the provider and the research institution are regarded as joint controllers. In such cases, the agreement must reflect this situation. See standards on this in [chapter 10](#).

For the sake of completeness: agreements on disclosure within one organisation may be laid down in institutional policy rather than in agreement(s). For example, the release of patient data from an UMC to researchers affiliated with the same UMC.

6 Rights of participants with regard to data and human tissue

[Participants](#) have several rights in relation to personal data and [human tissue](#). Every data controller must guarantee these rights and prepare policy to address them.

This chapter deals with the rights of participants, and how and under what circumstances they apply in health research. It builds on [chapter 3](#). In order to be able to exercise the rights at the research institution, the participant must first be informed, in accordance with [chapter 3](#), that the organisation is processing his/her data or human tissue. There are some exemptions to this obligation to inform. These affect the participant's rights to some extent. This is the case when the research institute cannot inform the participant because it has received the data in coded form. In a number of circumstances to be discussed below, it will not be possible to fully implement the rights of participants. These exemptions should be clearly defined in the policy and in information to participants.

6.1 Exercise of rights: when and through which party?

6.1.1 Participants may exercise their rights at the research institution to the extent that the latter can uniquely identify the potential or current participant.

6.1.2 If the research institution has only coded data that can be traced back to unique participants with additional information provided by the participant, it is important that the research institution specifies which additional information can uniquely identify participants.

Exercise of participants' rights at the research institution by providing additional data

If the data controller only processes coded data in such a way that participants cannot or can no longer be uniquely identified, the basic principle is that participants cannot exercise their rights with the data controller. However, data controllers (e.g. registries) may have set up their data processing in such a way that it may still be possible to uniquely identify participants after the provision of additional data. In that case participants can still exercise their rights at the research institution. It is important that organisations/processing departments draw up a clear policy and clear information about this. This will avoid uncertainty for participants when exercising their rights and prevent unnecessary procedures at the research institution.

If participants can still be uniquely identified after additional data has been provided, the person responsible for processing must clearly state what additional data is needed. If the participant cannot be identified in that way and thus personal identification is excluded, this should also be stated.

6.1.3 If potential and current participants cannot be uniquely identified by the research institution, they cannot exercise their rights at that organisation. The research institution will have to clearly indicate this on the website for each study (or research registration). The research institute should refer [data subjects](#) who have questions about whether their data is being processed to possible providers.

This applies to research or a registration in which the research institute only has access to coded data, which cannot be uniquely traced in the research data even with additional information. It is important that the research institute provides clear information on which rights can be exercised in such cases. In the case of [data that have been coded only once](#), a participant can withdraw his or her consent via the provider, but the other rights cannot be exercised via the research institute. After all, there is no technical possibility for the research institute to link information back to the provider at the personal level. In such a case, the rights can be exercised with the provider with regard to the data which have been processed by it or which have subsequently been provided to the research institution. If the provision takes place on a regular basis, this can have an effect on the research data.

6.2 Right of access

6.2.1 The participant is entitled to access the personal data processed about him or her. The controller must comply with this request, unless access may affect the integrity of the study.

In observational research, access will not affect the integrity of the research. In intervention studies, however, this may be the case if and for as long as data have to be processed in a blinded fashion. In this case, access is only possible after the participant has withdrawn from the study, or after the study has been completed.

6.3 Right to rectification

6.3.1 The participant has the right to the rectification of incorrect data if these are factually incorrect and the data processing may have consequences for the participant. The data controller should make this possible. In other situations, it is up to the researcher to assess whether rectification is necessary and possible, taking the integrity of the research data into account.

In therapeutic research, for example, data processing may have consequences for the participant. Under certain circumstances, this also applies to the later phases of research into the development and application of artificial intelligence in health care. As a rule, this involves research that is subject to the WMO. Take into account the requirements for data integrity. These follow from guidelines for good clinical practice.

In practice, if data originates from a provider (in case of [secondary use](#)), a correction of the source data may have an impact on a subsequent data delivery for the study.

6.4 Right of erasure

6.4.1 The participant has the right to the erasure of his or her data. The controller must comply with this request unless there is a legal obligation to process, or the erasure threatens to make the research impossible or seriously jeopardise it, or the processing is necessary for the fulfilment of a task in the public interest. Treat a data erasure request either as a withdrawal of consent ([section 4.8](#)) or as an objection to processing ([section 6.6](#)).

6.5 Right to data portability

6.5.1 The participant has the right to have the data collected from him/her transferred and, as far as technically possible, to have it transferred directly to another party, unless this may affect the integrity of the research.

In the case of observational research, exercising the rights of access and portability does not compromise the integrity of the research data. In intervention studies, this may be the case when data have to be processed in a blinded manner. In that case, transfer of data is only possible after the participant has withdrawn from the study, or after the study has been completed.

The request for transfer is usually a request for a copy of the data for the participant. Transfer can also mean that the participant requests that the data be given to another party. In both cases this does not automatically mean that the data may no longer be processed at the research institute. This is only the case if the participant also withdraws consent for (or objects to) data processing, or requests that the data be deleted.

Provide such data in an appropriate standard format (legally: 'in a structured, commonly used and machine-readable form'). Explain how the data should be interpreted or refer to existing explanations. Direct transfer to another party could include, for example, transfer to a digital personal health platform (PGO).

Formally, this right only relates to data provided by the participants themselves (e.g. through questionnaires, apps or sensors) and for which consent has been given. If feasible, it is advised to facilitate the request of participants who also want to receive derived data, such as genetic data or MRI images, or participants whose data are processed on another basis.

6.6 Right to object

6.6.1 The participant has the right to object to the processing of his or her data and human tissue for research purposes.

If the participant objects to the processing of his or her personal data, data must be deleted from the research database and human tissue destroyed, unless they are still retained or processed:

- a. for the purpose of verification or validation of previous research results;
- b. if there is a legal obligation or other reason and legal basis to retain them, or there is a legal exemption to the right to object; *or*
- c. if there are other compelling reasons why erasure threatens to make the research impossible or seriously jeopardise it. This does require a concrete, specific substantiation. Think for example of a substantial risk of distortion of the results that cannot be corrected and would make the results unreliable.

Inform participants to whom this relates of the reason for continuing to process the data or the human tissue. If informing them personally is not possible, as in the case of one-way coded data, this can be done via one's own website or the website and/or the general privacy statement of the research institute.

6.7 Dealing with individual findings

6.7.1 Inform the participant about the possibility of research involving individual findings and how they will be dealt with. The participant must give separate consent for research with a significant risk of individual findings (see [section 4.4](#)).

6.8 Responsibilities for institutions

6.8.1 Establish a policy on what information a person may need to provide in order to be uniquely identified in a record of coded research data in order to exercise their rights in relation to the data. Such a policy may also conclude that the registry cannot reasonably uniquely identify participants without the possibility of mistaken identity.

6.8.2 Make this policy available on the website. Refer to it in the information for those involved ([chapter 3](#)). Name the contact person to whom someone can turn if unique retrieval is possible and indicate which data the person must submit for this purpose.

6.8.3 Establish general policies on dealing with participants' rights in relation to research data. Have internal procedures in place to deal with requests. Involve the DPO in this policy. Specify clearly whom the participant should contact to exercise his or her rights.

6.8.4 Where relevant and appropriate, organise a system whereby the participant does not have to request access to data, but can do so via a secure portal. Consider, for example, a cohort of volunteers whose communication data is also available, such as the Netherlands Twin Register.

6.8.5 Establish rules on when the transfer of data to another party at the request of a participant is technically possible ([section 6.5](#)). As far as possible, design the systems to allow this (although this also depends on the receiving party).

6.8.6 The participant must identify himself before exercising his rights. If the participant is provided with data, this must be done securely. Specify what the participant has to submit for this purpose and how any transmission takes place.

7 Publication

Standards on publications cover two aspects. Firstly, the duty to strive for publication of the results of [scientific research](#). Secondly, the principle of publishing results anonymously. This gives substance to general requirements of care for honest scientific research, and with it the basic principles of data protection, such as lawfulness, fairness and transparency.

7.1 Publish the results of research

7.1.1 In line with the principles and standards of scientific integrity, publication of research results is the starting point. In that context, make research and [research data](#) as accessible as possible.

7.1.2 Observe the principles set out in the [CCMO memorandum on publication policy](#) for research that is subject to the WMO. Do this also where they apply to collaborations in non-WMO research.

Research subject to WMO

The [CCMO memorandum on publication policy](#) provides basic principles for the publication of results of research that is subject to the WMO. Among other things, the results of scientific research should be published without restriction. Agreements on publication or disclosure between the sponsor and the investigator should be transparent and laid down in advance in the [research protocol](#). In principle, these starting points also apply to collaborations in non-WMO research (to the extent applicable).

Additional transparency and publication requirements apply to pharmaceutical research that is subject to the WMO. For more information, see [the CCMO website](#).

7.2 Publishing information about patients or participants

7.2.1 Ensure that information about patients or [participants](#) is, in principle, anonymised in scientific publications or presentations.

Make sure that it is reasonably excluded that patients or participants can be recognised, spontaneously or through linkage with other information, by other people than the doctor or researcher involved.

7.2.2 Only include identifying information in publications if this is necessary from a scientific point of view. Ask the participants in question or their legal representative(s) for explicit consent, unless this

is practically impossible. Consent from a participant is not a licence to publish all identifying information.

7.2.3 If asking consent is impossible because the patient or participant has died or moved to an undisclosed destination, and complete anonymisation is also not possible, carefully weigh the interests at stake in that case.

Take the following factors into account:

- The period that has elapsed since the death of the [data subject](#);
- The scientific or other interest served by publication of the case in not completely anonymised form;
- The sensitivity of the data;
- Any evidence that the data subject would have objected to publication;
- The wishes of the living relatives of the data subject (after they have been informed of the intention to publish).

Seek advice from an ethicist or an ethics committee if necessary.

Exemptions to the principle of publishing anonymously, e.g. in case reports

Anonymisation of patients or participants is not always possible in clinical case reports. For example, if certain details are crucial for a good understanding of the case. In such cases, the main rule is that patients or participants, or their legal representatives, grant consent for publication. If the patient or participant has died and can therefore no longer be asked for consent, publication is possible in exceptional cases. The decision is up to the physician-investigator. International medical journals do sometimes require [\(substitute\) consent from the next of kin](#).

7.3 Disclosure of research data

7.3.1 Make research data public only in [anonymised form](#), unless participants have given specific and explicit consent for non-anonymised data to be disclosed.

In doing so, take into account the possibility of file comparison and foreseeable technological developments that may facilitate identification.

Open data

Obligations to publish open data may, under certain conditions, extend to publicly funded research. Developments in research and data management play a role in this (think of the FAIR principles for *data stewardship*), but also new regulations (the European Open Data Directive) and requirements of research financiers. The starting point for publishing open data is that data should be fully anonymised. Extra attention for anonymisation and statistical disclosure control is necessary, because in principle publicly available data can be used by anyone, and attempts at deduction or comparison cannot therefore be excluded. A [recent report by the WODC](#) contains an overview of guidelines and recommendations.

If anonymisation is not possible, data can be made accessible for re-use in other ways (see [chapter 9](#)).

7.3.2 When publishing results and making research data public, also take into account the recognisability of healthcare workers and healthcare providers. The starting point is that they cannot be separately identified in the results and data.

8 Management and archiving

This chapter deals with a number of rules for the management and archiving of personal data and [human tissue](#) for [scientific research](#). It implements the principle of storage limitation for health research in connection with aspects such as the responsibilities of the [controller](#) and information for [participants](#) which are also dealt with elsewhere in this Code of Conduct.

8.1 Safeguarding responsibility for management

8.1.1 Carefully manage and archive data and human tissue.

8.1.2 Ensure that the responsibility for data management is secured. For example, appoint one or more [administrators](#) and institutions.

8.1.3 Where relevant, provide access or issuance policies. Ensure that attention to data protection is guaranteed.

Safeguarding the responsibility for management is part of the agreements on controllership (see chapter 12). Within organisations, the management of data and human tissue is usually assigned to, or supported by, specialists or departments. Management or archiving of the data can also be entrusted to other organisations, such as the KNAW institute [DANS](#). In the case of research carried out under the responsibility of institutions to which the Public Records Act applies (including universities and UMCs), additional conditions apply for data management under the *Archiefwet* (Public Records Act).

Data and biobanks usually have access policies that include a role for a Data Access Committee (DAC). For an example, see [the generic access policy for access to and sharing of COVID-19 data of Health-RI and NFU](#).

8.2 Defining retention periods

8.2.1 For each study or data collection, define a maximum retention period in the [study protocol](#), [data management plan](#) or management regulations. Document the justification for the chosen period.

8.2.2 It is also possible to periodically review whether further retention is still necessary. Record such a periodic review. A legal obligation to retain or a fixed period in the protocol or in the information for participants has priority over periodic testing.

In determining the retention period, take into account (as appropriate):

- Legal retention periods:
 - For clinical drug trials: at least 25 years;
 - For research with advanced therapeutic medicinal products (ATMPs): at least 30 years;
 - For institutions to which the *Archiefwet* applies (including universities and UMCs): as laid down in selection lists;
 - Any legal retention periods that apply for a purpose other than scientific research;
- Guidelines for retention periods of relevant disciplines, professional groups and regulators;
- Insurance retention periods (e.g. in the case of research that is subject to the WMO);
- Institutional policy of the administrator;
- Possible replication and validation of research, including due to retention periods required by scientific publications; *and/or*
- Use and re-use for future scientific research.

The [CCMO](#) and ELSI Servicedesk provide more information on retention periods for medical and health research. The CCMO considers a storage period of fifteen years acceptable, provided it is substantiated in the research protocol. If a shorter or longer retention period is sufficient for a specific study, the CCMO considers this to be the most suitable, provided it is substantiated.

Disciplines and professional groups can provide further guidelines and justification for retention periods. In addition, institutions can lay down and substantiate standard policies for types of research. Individual research projects can build on this.

Many medical/scientific journals require a data availability statement for publications. Journals can also require a minimum retention period as part of this. A retention period of at least ten years for the source data on which the results are based is customary.

8.3 Appropriate safeguards for archiving

8.3.1 Pay attention to appropriate safeguards when archiving data after the end of the research.

For example, delete communication data as soon as they are no longer needed. [Anonymised](#) data may be kept longer than the specified retention period, unless otherwise agreed with participants (see [norm 5.7](#)). Additional rules apply to anonymised human tissue after the WzI comes into force.

8.4 Responsibilities for institutions

8.4.1 Provide a research infrastructure in which the proper management of data and human tissue is the rule and is facilitated.

8.4.2 Ensure that the responsibility for data and human tissue management is clearly assigned within the organisation, for example in general management regulations.

Pay attention to, among other things:

- Data security and protection;
- Informing and exercising the rights of participants;
- Compliance with retention periods and standard retention periods used for certain types of research;
- Access policy: agreements on making available and/or granting access to data and human tissue for research purposes;
- Where applicable: the handling of individual findings; *and*
- Deleting and supervising the deletion of the data after expiry of the retention period.

Other legal frameworks may impose additional conditions for data and human tissue management. In the case of research conducted under the responsibility of institutions to which the *Archiefwet* applies (including universities and UMCs), additional conditions apply to data management. The WzI will set additional rules for the management of human tissue. Among other things, human tissue managers must ensure that management regulations are in place.

9 Use and re-use of research data and human tissue for new research

Data or [human tissue](#) previously obtained or processed for research is often (re)used for [new scientific research](#). From the point of view of scientific integrity, the basic principle is that [research data](#) should be made available 'as openly as possible, as closed as necessary'. Researchers are expected to cooperate in making the data they have collected and used findable, accessible, interoperable and reusable, where appropriate, in accordance with the FAIR principles.

Two situations can be roughly distinguished in this respect. The first is when researchers, in the context of a new study, want to 're-use' data and human tissue that was collected and used in a previous study. An example is the re-use of data from a completed clinical study for follow-up research. A second situation – increasingly common – is that researchers want to use data and human tissue from a data or biobank for research purposes in the context of a study. Researchers then request that data and human tissue be 'issued' to them. The manager will then assess whether the purpose of the specific study fits in with the generally broader purpose of the biobank. One example is human tissue and related data for a study of heart failure, from a biobank that was set up in the context of cardiovascular diseases.

The (re-)use of data and human tissue for new scientific research must of course comply with the applicable laws and regulations and ethical principles. This means that the standards formulated in earlier chapters also apply here. What this exactly means in the context of re-use or issue is explained in this chapter.

9.1 Anticipating use and re-use for future research

9.1.1 Before collecting or processing data or human tissue for research, consider whether it is appropriate to make it available for (re-)use in future scientific research. If so, make preparations for this and take it into account in the design and organisation of the research.

Please consider the following points:

- In the [research protocol](#) and [data management plan](#) (see [section 1.1](#)), establish if and how data and/or human tissue can be used for future scientific research;

- Inform [participants](#) about the possibility of this (re-)use. If necessary, ask consent for this separately (see [section 4.4](#)). Inform participants of their rights and how to exercise them ([section 6](#));
- Ensure that data and human tissue are properly managed, and clarify how and by whom a request for re-use is assessed (access to or sharing of data, or issuing of human tissue, see [chapter 8](#)); *and*
- Take (re-)use into account when determining the retention period ([chapter 8](#)).

Make sure that participants are adequately informed of the purposes and conditions under which future research will be conducted. Always ask consent separately for re-use of data or human tissue for future research if the collection and processing are primarily aimed at a specific research question, as in research that is subject to the WMO. Possible re-use should be justified in the research protocol and fit in with the purposes and conditions of the original research (see also [chapter 1](#) and [chapter 5](#)).

If data or human tissue has already been collected and/or processed for future scientific research or use in different studies, for example when setting up a biobank or registry, make sure that participants are informed about this and that the consent is tailored accordingly (see [chapter 3](#) and [chapter 4](#)).

9.2 Complying with data protection rules for use and re-use in new research

9.2.1 Ensure that a concrete proposal for the (re-)use of data or human tissue complies with the data protection rules and conditions of this Code of Conduct.

The conditions of other chapters apply accordingly. An essential question is whether the research is possible under the conditions of the previously given consent or the previously offered option to object ([chapter 4](#) and [chapter 5](#)). In doing so, please consider the following points for each individual data source.

If participants have given their consent to the purposes: does the research fit within the purposes for which participants gave their consent? If the purposes of research and processing of data and human tissue were not fully defined at the outset, have they been or will they be further specified where necessary ([section 4.5](#))?

If the processing was previously subject to an exemption to the principle of consent: do these exemptions also apply to the new research? For research for which data or human tissue is re-used and for which no consent was initially sought ([secondary use](#) situations), the conditions from [chapter 5](#) must also be met.

Are participants adequately informed about the research and the conditions under which data or human tissue will be processed? Also consider the information and control options offered to participants after consent was given (see [section 4.5](#)). If more information or control options should be offered to participants, assess whether participants can or should be informed individually about the research and under what conditions (see [section 3.2](#)). Exemptions to the basic principle of consent affect this, such as whether participants have died (see [section 5.4](#)).

If the above cannot be met, data or human tissue can only be (re-)used for new research if participants can and may be approached about it ([section 4.1](#)) and give their consent again ([chapter 4](#)), or if the data can be [anonymised](#) for the purpose of research ([section 8.3](#)).

It makes sense that this should be tested for legitimacy before each new study. This is the responsibility of the [provider/manager](#). Depending on the provider or data source, a particular assessment procedure applies ([chapter 8](#), see also [section 5.7](#)). This assessment can be carried out by an ethics committee, a *data access committee* and/or an administrator.

9.2.2 When making data or human tissue available for (re-)use in new research, also take into account the rights previously exercised by participants (see [chapter 6](#)).

Please consider the following points:

- Data from participants who have objected or withdrawn consent to use their data may not be (re-)used for new research.
- Data from participants who have indicated that they do not wish to be contacted again for follow-up research can only be used if they have not withdrawn their consent and (re-)use fits within the purpose under which they previously consented ([section 4.8](#)).
- The same applies to data of participants who have not responded to a contact request, for example to complete a new questionnaire ([section 4.8](#)).

10 Controllershship

In the preceding chapters, the standards of the Code of Conduct have been drawn up to guide researchers and providers in complying with and organising data protection in health research. Formally, compliance with the GDPR rests with the controllers to whom researchers and providers are bound. This chapter describes the role of a data controller in health research. It also describes related roles, such as that of processor, and explains how the distinction between such roles can be safeguarded. Chapter 10 discusses how data controllers can implement the standards in the Code of Conduct and ensure compliance.

The subject matter in this chapter is complex. Health research often involves several parties in different roles, and the legal issues are very complex. There is usually a chain of processing and cooperation during research. It is important that the responsibilities for data processing are clearly assigned within this chain.

This chapter explains those responsibilities in GDPR terms for a number of common situations. It is intended as an introduction for researchers. In case of doubt, always consult your [DPO](#) or legal support. This also applies to collaboration or consortium agreements. Cooperation in research will always have to be set out in an agreement. That is the work of specialists. See the last norm of this chapter.

Whereas in other chapters legal 'jargon' was avoided as much as possible, here it is unavoidable to use some basic GDPR terms. These were already discussed in Chapter 2. The terms used in this chapter are briefly repeated below:

- [Controller](#): the person or organisation who determines the purposes and means of data processing;
- [Processor](#): the entity that processes personal data on behalf of the controller.

See the list of definitions for the full definitions. This chapter also builds on [the Reading guide](#), in which the concepts of [healthcare provider](#), [provider](#) and [research institute](#) are discussed in relation to each other. When this chapter refers to responsibility or processing, this means 'controllershship' and 'data processing'.

10.1 Main rule: when does one become a data controller?

10.1.1 The research institute associated with the researcher who prepared the [research protocol](#) is the data controller of the research data.

Note: Sometimes one can be a data controller without having access to the personal data oneself. For example: a research institution commissions a survey bureau and has determined which data must be specifically requested from which respondents. Then the research institution is the data controller for that survey, even if they only receive the aggregated results.

10.1.2 If the research protocol has been drawn up by a doctor who is not employed by a healthcare provider but by a medical specialist company, then, in principle, this doctor is the data controller.

10.1.3 However, if this doctor is bound by the institution's policy in respect of [scientific research](#) and/or relies heavily on the ICT department or other support for the research provided by the healthcare institution, such as nurses, then the doctor and the healthcare provider are jointly responsible for the processing of the data.

The latter will generally be the case with most healthcare providers.

10.2 Joint controllers

10.2.1 If researchers from different research institutions have worked on the research protocol, they have jointly determined the purpose and the means. In that case those research institutions are jointly responsible for the data processing.

Joint controllership means, with regard to data protection, that good agreements must be made about the division of responsibilities (see also norm 10.2.3).¹⁵

Joint controllership can also arise in other forms of close cooperation and interdependence in a study. For example, a joint platform can be set up to analyse [research data](#). And a joint decision can be made as to which researchers can make use of this platform and under what conditions.

In the Netherlands, research that is subject to the WMO is always based on joint responsibility between the researcher (sponsor) and the investigator (with whom the principal investigator is associated). The latter does more than just make the data available (see the following norm), he actively cooperates in implementing the protocol. He also has access to the data for his own publications. Incidentally, this

¹⁵ Naturally, other agreements are made in the cooperation or consortium agreement, such as those concerning finances, intellectual property rights, etc. This falls outside the scope of this Code of Conduct. See further [section 10.5](#).

view does not seem to be shared in all countries. The CCMO model agreement also makes the reservation that this may be thought of differently at a later date.¹⁶

Note: Joint controllership does not mean that each party is now fully responsible for all data processing by the other parties. Each party is only responsible for the processing of data that coincides because of the joint purposes and means. For example, in the case of joint research, each party has its own research data. Some of it is provided for the purpose of the joint project. The parties are then jointly responsible for processing all data submitted for the purpose of the joint research. But one party does not become responsible for processing the *original* data of the other parties.

For researchers, it can be difficult to determine when there is joint controllership and when there is another form of collaboration. Because collaboration between different parties must always be given shape in a collaboration or consortium agreement or a Data-Sharing Agreement or a Materials and Associated Data Transfer Agreement, the lawyers or the [DPO](#) must determine this together with the researchers involved. The following situations can be distinguished:

- a. Data is transferred from one controller to another;
- b. The parties are jointly responsible for processing;
- c. Processor (see below);
- d. One of the parties merely offers a supporting role, such as advice on the design of an analysis platform or legal advice, without processing personal data of [participants](#).

In the last case, the role does not fall under the GDPR; in the other cases, it does.

10.2.2 Joint controllership does not arise between provider and research institution if the provider's role is limited to sending invitations to participate ([chapter 4](#)) or provision of data and/or human tissue for secondary use as specified in [chapter 5](#).

In that case, the provider did not help determine the purpose and means of the data processing. Therefore, a data provider does not automatically become jointly responsible for data processing when he cooperates in a study. This only happens if the provider is also involved in drawing up the research protocol, or if he has his own interest in the data processing. The latter can be the case if the provider has access to the research data and can use it for his own research. If the parties are not jointly

¹⁶ <https://www.ccmo.nl/onderzoekers/publicaties/formulieren/2018/12/18/k3-model-onderzoekscontract-clinical-trial-agreement-bedrijfsgeinitieerd-onderzoek>

responsible for the processing, the provider is of course solely responsible for processing the data and human tissue supplied, and the processing that precedes this.

Sometimes this provision is done through a [TTP](#) that ensures that the data is [pseudonymised](#). This TTP then acts as a processor for the provider (see the next norm). This is no different if the TTP is paid by the research institution for its services.

10.2.3 If data controllers are jointly responsible for research, they should make clear, transparent agreements on how they will interpret and divide these responsibilities among themselves. This applies in particular to their obligations and responsibilities towards participants.

Among other things, data controllers must agree which DPOs will act as contact persons, and to whom participants can turn to exercise their rights. Participants must also be informed about this (see [chapter 3](#)).

10.3 Processors

10.3.1 A processor may be involved in the research. The processor is always commissioned by the person responsible for processing. In the case of health research, this is either the client of the provider, or the research institute, or both (if both are responsible for processing). The processor therefore does not need a [basis](#). The basis for processing rests with the data controller(s).

Examples of processors are a mail house that sends out invitations, a TTP that pseudonymises the data, a contract research institution that works on behalf of the sponsor of a trial, or a cloud service that processes the data.

A processor in the sense of the GDPR is always a third party with respect to the controller. Within a large organisation, there are usually various processing activities, often spread across multiple departments. This does not automatically make one department a processor for another. Departments within the same organisation are not different parties in the sense of the law.

As an aside, the fact that units within a large organisation cannot, in principle, act as processors for other organisational units does not mean that no agreements must be made internally. It follows from the GDPR in general that there must also be internal compartmentalisation, and that there must be a register of the various processing activities. This is part of the general implementation of the GDPR and is not specific to a research institution. It therefore falls outside the scope of this Code of Conduct.

How a researcher can contribute to the register of data-processing operations has been discussed in [section 1.3](#).

A researcher who is involved in the implementation of the research protocol as an employee of the controller cannot analyse data for the purposes of the research in the role of a processor.

As noted, a processor works on behalf of a controller. However, health research, like any scientific research, requires a certain independence of the sponsor. Otherwise the conditions of the Code of Conduct for Scientific Integrity are not met. The processor's role excludes this scientific independence. Of course, this does not mean that the sponsor cannot play a role in determining the research purposes, the budget and the means. But the goal can never be a certain outcome, and the researcher must be allowed a certain amount of freedom when working out the means. Processors do not have that freedom. Contract research in which this independence is not guaranteed cannot be regarded as scientific research in the sense of this Code of Conduct.

This does not mean that a processor cannot use scientific methods. For example, a processor can select certain data for certain characteristics, so that the research institution only receives data that are necessary for the research. This may require substantive scientific knowledge. This is the case, for example, when images are analysed and converted into annotations on behalf of a research institution. The research institute has then still determined the goal and the essential means. As soon as there is involvement in the analysis of research data, this can only be done as a researcher. More specifically and legally speaking: as an employee of a research institution that has a basis to process that data for health research.

10.3.2 The provider must also be able to base the provision on a basis. Therefore, the provider cannot circumvent the conditions for [secondary use](#) ([chapter 5](#)) by acting as a processor of the research institution.

The grounds for processing for secondary use by the provider were discussed earlier. It is not entirely inconceivable that the research institution has a basis, but the provider does not. For example, if the research institution has consent as a basis and wishes to receive data from a provider, the consent must also extend to allowing the provider to supply the data. (See [chapters 4](#) and [5](#).)

10.3.3 The research institution itself needs a basis for processing personal data for health research ([chapter 4](#) and [section 5](#)). The research institute cannot carry out this research in the role of processor of the provider. This has an effect on the researchers affiliated with the research institute.

10.4 Securing distinction between different roles within one organisation

10.4.1 A research institution can also fulfil the role of processor under certain conditions. However, these roles must be strictly separated through technical and organisational procedures.

It is permissible for a department of a research institution to receive personal data from a providing organisation to process them on its behalf in such a way that they can be analysed by researchers for the study. For example, by removing [directly identifying data](#) and other data not relevant to the study, which the providers or their regular processors (for example, the supplier of a healthcare information system) are technically unable to do. That provider will then remain responsible for processing the research data to be provided.

In that case, so-called 'Chinese walls' must exist between the two distinct processing operations within the same organisation. In other words: between where one acts as processor of the provider, and where one acts as processor of the research institution. The term 'Chinese walls' comes from the compliance literature, particularly around financial transactions to prevent conflicts of interest. This is applied accordingly here in the context of data protection.

A 'Chinese wall' requires strict separation between the types of processing:

- a. A separation at the level of the data infrastructure, for example by separate databases or partitioning within a database with non-overlapping access rights;
- b. An organisational separation, for example by assigning the roles to different departments;
- c. A separation of personnel, i.e. no exchange of personnel between the different departments, in this case the department acting as processor and the department where the research is carried out (for the separation of personnel, see also [section 10.3](#)); *and*
- d. Internal supervision, in the financial world a 'compliance officer'. Here it would be the DPO.

These points should be elaborated and documented by the research institution. In the event of an investigation by the Data Protection Authority, it must be possible to demonstrate that the research institution does indeed have such 'Chinese walls'. Points b and c above can be problematic if ICT staff work for both departments. An additional confidentiality agreement is then necessary. This should not only imply, as usual, that the ICT staff will not disclose data from the research institution, but also that they will not use data from the role of processor in the role of data controller. Preferably, a separation is also made in the direct management. A researcher connected to the research institute can never fulfil both roles at the same time in a particular study. In other words, the researcher who ultimately

analyses the data for the purposes of the study should not have had access to that data first in the role of processor or be able to access the data obtained by the research institution in the role of processor.

The situation in which medical researchers conduct research with data (and/or human tissue) of patients with whom they have a treatment relationship must be distinguished from this. In this case, there is no separate providing organisation which orders the research institution to transform the data of this organisation into research data to be supplied in the role of processor. The provision to the physician-investigator takes place internally. Physician-investigators combine a role as provider at the research institution with a role in research. This combination of roles is possible. However, these roles should be kept as separate as possible, including ensuring that research data are processed in an unidentifiable way ([chapter 2](#)). The conditions under which medical researchers may access data of participants with whom they have a treatment relationship are detailed in chapter 5 ([section 5.7](#)).

10.5 Defining roles in agreements

10.5.1 The collaboration on data processing in the study should be laid down in clear agreements between the institutions and data controllers involved. Consult the DPO or legal department of the research institute.

Drafting contracts is specialist work. For example, lawyers will want to build on the European Data Protection Board (EDPB) guidelines on processing agreements and joint controllership. They will also want to connect as much as possible to existing examples or models where these are applicable. In the case of joint controllership, it is recommended that a diagram be drawn up to show which part of the data processing in the chain the parties are jointly responsible for, and which parts each party is independently responsible for. This diagram can be included in an appendix to the agreement.

It is of great help to specialists if there is a good description of the planned research, the envisaged role of each of the parties, and how and via whom the data flows will be channelled. This is beneficial to the timeframe of the drafting and the quality of the agreement.

11 Assurance, monitoring and implementation

In the process of developing the Code of Practice, a wide range of parties involved in health research were consulted through consultations and mutual dialogue. Their input has been used to develop an adequate framework of standards that is ethically and socially acceptable, sufficiently workable for researchers and institutions, and in line with the legal frameworks for data protection.

This chapter discusses a number of general responsibilities that institutions have for ensuring compliance with the Code of Conduct. It also discusses the monitoring of compliance and further development.

11.1 Security

11.1.1 Draw up an institutional policy for data protection in research. Include the rules from this Code of Conduct. Make sure there is room for research that complies with these rules.

11.1.2 Make data protection policies and facilities, and how data may be processed within the research institution, transparent and easy to apply in researcher practice.

11.1.3 Make sure the [DPO](#) is easily accessible for researchers. If the DPO works in a large organisation where health research is also carried out, but not as the main mission, make sure the DPO also has staff available to advise on health research. If the DPO is supported by 'privacy officers', let them work as a team (see also the following standards).

Note: the appointment of a DPO and how his position in the organisation must be safeguarded follow from the general GDPR standards and are not elaborated on in this Code of Practice. It follows de facto from the GDPR that every research institution must have appointed a DPO. This also applies to healthcare providers.

11.1.4 Provide adequate support for data protection in health research. This should be in addition to, and consistent with, support in relation to data stewardship and methodological aspects.

It is also recommended that the research institution should organise a one-stop shop where researchers can ask questions about the design and implementation of health research. Currently, lawyers, the contract/technology transfer office and the DPO within one organisation sometimes give different signals. A one-stop shop could prevent this.

11.1.5 Ensure an organisational culture that pays attention to data protection and that sufficient knowledge and skills are available in this area.

Invest in training and education on data protection for both researchers and research assistants, also with regard to terminology. For example, researchers tend to use the term "[anonymous](#)" when data is perceived by them as anonymous, while formally the data has [been pseudonymised and is therefore still personal data](#).

11.1.6 Ensure that complaints about breaches of this Code of Conduct become part of the general complaints and reporting procedures about the processing and provision of data and human tissue in or for health research. Breaches of this Code of Conduct must be met with appropriate sanctions. These must be in line with, and proportional to, the related breaches of scientific integrity (possible and actual), the GDPR, related laws and regulations and, where applicable, the Wkkgz.

11.2 Monitoring compliance with the Code of Conduct

11.2.1 Establish institutional policies and procedures for review and assessment of research involving personal data and human tissue. Make sure that compliance with the rules from this Code of Conduct ([section 1.4](#)) is also checked in the process.

The Code of Conduct will play a role in the assessment of requests for providing and processing data and human tissue for research by ethics committees and *Data Access Committees* (as was the case in the previous codes of conduct). Focussing on proportional review and assessment of research is recommended, which is in line with policy and procedures for quality assurance ([section 1.3](#)).

In addition, the Code of Conduct will play a role in the awarding of grants by Dutch subsidy providers.

11.3 Implementation and further development

The Code of Conduct provides a general guideline for dealing with data protection in health research. It will have to be implemented in all areas and elaborated in certain parts. This is an ongoing process that can tie in with the many things that are already happening in the field, such as through Health-RI and its [ELSI Service Desk](#).

The implementation process is beyond the scope of this Code of Practice. This also applies to the further development of data protection where this code of conduct offers basic standards, such as the

necessity and execution of a [DPIA in health research](#). The basic standards in this Code of Conduct already offer sufficient clarity for the field to work on.

The experiences with compliance and implementation and needs for further development of the Code of Conduct will be evaluated after approximately two years on the initiative of COREON, in consultation with other field parties.

Part 2

Legal justification

Explanation of the legal justification

The explicit purpose of the Code of Conduct is to elaborate the complex legislation and regulations on data protection in health research into a set of concrete standards for Dutch health research that are accessible to researchers. During the reading sessions with researchers, it became apparent that it would be confusing if a legal justification/substantiation of these standards (the why) was included in the same chapter. It was therefore decided to deal with the legal justification separately.

The members of the core group were directly involved in the formulation of the core standards and agreed with them. During the discussion, the legal and ethical provisions and principles applicable to health research were taken into account. The legal justification is the result of those discussions. It describes which provisions of the relevant legislation form the basis of the Code of Conduct. Where the provisions offer room for different interpretations, ethical principles have been complied with to offer a responsible balance, in the opinion of the authors, between the social interests served by health research and the interests of those involved whose data may be relevant to health research or to the participants once the data have been processed in health research. It should be noted that the Code of Conduct adheres to the current statutory frameworks. Bottlenecks arising from this cannot all be resolved with a code of conduct.¹⁷

The legal justification is not meant to be read as a stand-alone document. The standards are not repeated here, nor are the definitions and abbreviations used. Please refer if necessary to Part 1, the main standards of the Code of Conduct.

The legal justification has been drawn up by the MLCF team (in particular, Evert-Ben van Veen and Martin Boeckhout). Several members of the Core Group (in particular, Paul Dalhuisen and Michel Paardekooper) acted as sounding boards.

¹⁷ For a perspective on the obstacles in legislation and regulations, see among others [the ambitions for an agreement system of Health-RI](#) and the [concerns of FMS, NFU, COREON and Health-RI about the fragmented legal framework for the \(re\)use of body tissue](#).

Introduction

In the part addressed to researchers and data controllers, the aim has been to formulate the standards that:

- are legally conclusive according to European and Dutch law;
- are ethically justified; *and*
- are as understandable and workable as possible for researchers and research institutions.

This legal foundation describes for each section:

- which provisions of the relevant regulations are elaborated and fleshed out;
- what legal basis this elaboration is based on, and
- -when applicable- the arguments on the basis of which further choices or interpretations were made in appropriate cases.

The legal foundation follows the same structure as the Code of Conduct itself. This means it does not follow the structure of the GDPR rigorously but rather the so-called *data life cycle* of research data and human tissue. An [appendix](#) provides a section-by-section overview of the legal provisions dealt with in the GDPR, UAVG and other important pieces of legislation (in particular, the Wgbo and WzI). It should be noted that the Bill on the Control of Human Tissue (WzI)¹⁸ has not yet been debated by Parliament. The debate in the Lower House is in its initial stages. Amendments to this bill during the political process may have consequences for a number of provisions and their application in this Code of Conduct. For the sake of length and readability, articles of law are only referred to and not quoted extensively.

During the drafting of the Code of Conduct, an extensive consultation process took place among representatives of field parties involved in health research and researchers represented by COREON. In addition, a public consultation round was organised. The results of these consultations have been taken into account as far as possible. Appendix 1 to the main standards of the Code of Conduct contains a description of the process and how the results of the consultations were dealt with. The submitter believes the Code of Conduct has been made sufficiently representative for the field and can count on sufficient support elsewhere, in addition to an adequate explanation/specification of the applicable standards.

¹⁸ Bill on rules for actions with human tissue performed for purposes other than medical treatment or diagnosis of the donor (Human Tissue Control Act), Parliamentary Papers 35844.

Purposes

The part addressed to the researchers 'translates' the applicable regulations into standards that can be used by researchers. Where reference is made here to researchers, this also includes the data controllers to whom the researchers are linked. The consequences for the parties responsible for processing are dealt with in the practical part. In addition, the practical part contains standards and instructions for the so-called providers. As will be discussed below, these are the people, such as care providers and healthcare institutions, who make research data available to researchers.

The Code of Conduct explains and specifies the standards for data protection in health research. It not only covers the GDPR: it also specifies other legal frameworks (proposed and existing) relevant for data processing in health research, such as the WGBO, the UAVG and the WzI.

Scope

The Code of Conduct applies to the processing of personal data and human tissue, and in some respects also of data and human tissue of deceased patients, for scientific health research in the Netherlands.

This Code of Conduct applies a broad definition of *scientific research*, in line with the definition given to this concept by the CCMO.¹⁹ According to Recital 159, the concept of scientific research in the GDPR should be interpreted broadly. The starting point for the Code of Conduct is that if the concept is followed, the Dutch Code of Conduct for Scientific Integrity will also be observed.²⁰ This principle ensures that scientific research can contribute to an open and innovative society and serves the public interest, at least in this sense.²¹ Questions such as those raised in the Preliminary Opinion of the EDPS, about the fact that some data processing claims to be scientific research while only serving the interests of the data controller, and whether a justified appeal is made to the exemptions for scientific research in the GDPR, are covered by these integrity standards, in combination with the standards set by this Code of Conduct.²² This is also in line with an earlier opinion of the EDPB that the term scientific

¹⁹ This view follows from the CCMO definition of medical scientific research, see: Ministerie van Volksgezondheid 2005; Compare also: Nederlandse Gedragscode Wetenschappelijke Integriteit 2018, which defines scientific research as 'the quest for knowledge obtained through systematic study and thinking, observation and experimentation'.

²⁰ KNAW e.a., 'Nederlandse gedragscode wetenschappelijke integriteit', <https://easy.dans.knaw.nl>, doi:10.17026/DANS-2CJ-NVWU, 2018.

²¹ Certain health research must comply with a more specific interpretation of the public interest, see chapter 5.

²² European Data Protection Supervisor 2020.

research cannot be stretched beyond its usual meaning, which in this context is understood as a 'research project in accordance with the relevant methodological and ethical standards of the sector, and in accordance with good practice.'²³

The definition of *health research* is a comprehensive description of the subjects which the research groups and institutions affiliated to the COREON Foundation, the submitter of the Code of Conduct, work on and identify with. In this respect the Code of Conduct is sufficiently defined, even though one research group or institute may focus more on questions of disease and its causes, another more on the treatment of diseases, and yet another more on the functioning of the health care system.

The Code of Conduct deals with the anonymisation of personal data in a number of places. Anonymisation is a form of data processing that falls under the GDPR. However, the GDPR, and therefore the Code of Conduct, does not apply to the processing of data after it has been anonymised. Institutions that subscribe to this Code of Conduct are obliged to respect the conditions for scientific integrity, including for research with such data.

The scope of the Code of Conduct is more extensive than that of the GDPR in a number of respects. Firstly, medical confidentiality in the Netherlands continues after death. A number of rules in the Wgbo and the future WzI therefore also offer protection to a certain extent to previously collected data and human tissue *of deceased patients*.²⁴ This is reflected in this Code of Conduct.

Secondly, the handling of *human tissue* in research is inextricably linked to the processing of personal data. Human tissue is not personal data as such, but it is a potential carrier of information,²⁵ and personal data are often linked to it (in which case, it is identifiable human tissue under the WzI). Special conditions are attached to the collection and processing of human tissue. Related questions concern the protection of the rights and freedoms of individuals, because human tissue usually contains personal data. As noted, separate legislation - the aforementioned WzI - is being prepared for this.²⁶ The Code of Conduct takes this into account as much as possible. COREON also drew up the 'Code of conduct for the responsible use of body tissue in scientific research' (Code Goed Gebruik 2011). The present Code of Conduct, together with the WzI, replaces this earlier code. This is also an extension to the GDPR.

²³ European Data Protection Board 2020.

²⁴ Article 7:457 of the Civil Code.

²⁵ See also recital 35 GDPR.

²⁶ Bill on rules for actions with human tissue performed for purposes other than medical treatment or diagnosis of the donor (Human Tissue Control Act), Parliamentary Papers 35844.

The broadening compared to the GDPR as explained above is justified in a code of conduct under the GDPR, because a code of conduct must provide an 'explanation' from the perspective of data protection for all relevant standards for health research.²⁷ After all, even though the GDPR aims to provide a harmonised European legal framework for the processing of personal data, there is a lot of room for national legislation with respect to data concerning health and scientific research.²⁸ This must be taken into account in a national GDPR code of conduct.

Target groups

Formally, the parties responsible for processing data in health research are the addressees of the standards. These are the research institutions with which the researchers are affiliated and the so-called providers, which are often affiliated with individual care providers. As shown in Part 1, these roles can coincide. The research institutions subscribe to the Code of Conduct. However, as seen, the standards are primarily aimed at researchers. Where applicable, each chapter concludes with what the standards aimed at researchers mean in concrete terms for the data controller. By distributing the Code of Conduct to the researchers and especially by supporting them with its implementation, as stipulated in chapter 11 of Part 1, and with the appropriate supervisory mechanisms (see also chapter 11), the data controller can comply with the Code of Conduct. The Code of Conduct thus offers controllers an important instrument for complying with the "principle of accountability" that is expressed in various provisions of the GDPR (in particular Articles 5.2, 13 and 14 and 24 GDPR).²⁹

Comments on the content, application and scope of the Code of Conduct

As already indicated in the introduction to the standards, the Code of Conduct does not explain all applicable privacy regulations. It concerns explanations/specifications that are necessary for the sector, partly in connection with guaranteeing the rights of those involved. Examples of articles that

²⁷ Article 25 of the Personal Data Protection Act was explicit about this. The Dutch Data Protection Authority could determine that a code of conduct: "...constitutes a correct elaboration of this Act (being the WBP) or of other statutory provisions concerning the processing of personal data." (our emphasis)

²⁸ Cf. 9.2 h to j GDPR, Article 89.2 GDPR.

²⁹ On the principle of accountability see, for example:

<https://www2.deloitte.com/ch/en/pages/risk/articles/gdpr-accountability-principle.html> or
https://edps.europa.eu/data-protection/our-work/subjects/accountability_en

are only touched upon are Article 30 GDPR (the register of data processing) or Articles 33 and 34 GDPR (reporting a data breach).

The Code of Conduct distinguishes health research as standardised by this Code of Conduct from evaluation of the quality of care and quality registrations. The interpretation of the term 'health research' in this Code of Conduct can contribute to discussions about when this is scientific research. For example, health research aims to lead to new insights with a certain general validity outside the group of participants whose data were processed for the research. This is in principle not the case with quality improvement via benchmarking, although new patients will be able to benefit from the results of quality improvement initiated via a benchmark. Evaluations of the quality of care that also lead to general statements on improving the quality of care (or are intended to) may have to be regarded as scientific research and therefore also fall under the scope of the Code of Conduct, to the extent that patient data or human tissue is used in the process.

Furthermore, the Code of Conduct deals only roughly with specific forms of health research. This applies, for example, to research on children and adolescents up to 16 years of age. In the GDPR these are considered an especially vulnerable group.³⁰ They are represented by legal representatives (see further section 4.2). At the same time, it can be important in certain questionnaire studies that they are heard and feel heard, which may not always be possible to achieve through parental representation.^{31,32} How this balance can be achieved in Dutch health research is beyond the scope of this Code of Conduct.

³⁰ See Recital 38 and Article 8 of the GDPR.

³¹ Compare also Article 5 (5) UAVG.

³² For example: Konijnenburg, Teeuw & Ploem, *European Journal of Pediatrics* 2015/174; Liu e.a., *Journal of Adolescent Health* 2017/61; Flores e.a., *Nursing outlook* 2018/66; Bauman, Mellins & Klitzman, *The Journal of Law, Medicine & Ethics: A Journal of the American Society of Law, Medicine & Ethics* 2020/48.

Reading guide

This chapter introduces the terms that are essential for the researcher to read the Code of Conduct. As much as possible, the concepts known to the researchers have been used. A specific GDPR concept will only be explained if necessary, namely if that concept also plays a key role in the section of the Code of Conduct aimed at the researchers. This applies, for example, to the term processing. The following is a translation into GDPR terms that are not already described in the section addressed to the researchers. The other terms in the Guide are taken from the GDPR, sometimes abbreviated to keep them readable for researchers. This does not prevent a GDPR-compliant application of these terms.

- The term "participant"

This concept does not exist in the GDPR. A participant is of course a data subject in the sense of the GDPR, unless it concerns data about deceased persons or anonymous data. This is one of the reasons for using the term participant.

Besides the fact that participants can also be deceased, to whom the GDPR does not apply, there is another reason not to always use the term 'data subject'. It is not sufficiently distinctive. As will become apparent, a participant is the data subject whose data may lawfully be processed by the health research institution. However, health research also involves other data subjects who do not participate. Think of patients who are approached by their care provider for participation in research. Via an address provided in such a letter, a data subject, a potential participant in terms of the Code of Conduct, can register for and consent to data processing in the context of the study. Only after this has been done (according to the conditions set by this Code of Conduct) can one speak of a participant.

Specific legislation uses different terms, namely 'test subject' in the WMO and 'donor' in the WzI. Participant is used as an umbrella term. This concept fits in well with the language used by researchers and the communication surrounding research (such as: 'would you like to participate?').

- The concept of 'provider'

The GDPR does not recognise the term 'provider' as a noun. However, it does mention 'providing' as a verb.³³ This term has become established in health research. For example, it was used in the 2004³⁴ Code of Conduct. That is why it is adhered to in this Code of Conduct.

The provider need not coincide with a controller. This is due to professional confidentiality in healthcare. This does not apply to the person responsible for processing but to the care providers who are directly involved in the implementation of the treatment contract.³⁵ There must be a basis for that care provider to breach professional confidentiality by making the data available to a researcher. Although the care provider is always linked to a controller - unless he or she works alone - he or she also has his or her own responsibility, as disciplinary law shows.

If the data are transferred to a third party as referred to in Article 4.10 GDPR, the provider is always a data controller. According to the GDPR's system, the provision of data to a third party is carried out on behalf of the controller. But as Article 4.9 GDPR indicates, the provision of information can also take place internally within the party responsible for processing. For example, from the care provider to the researcher within that party responsible for processing. This is another reason that the provider can be either a natural person, i.e. a care provider to whom professional confidentiality applies, or a legal entity, i.e. the party responsible for processing.

For the record, the provider may also be a research institution that provides data to another research institution.

As stated in the introduction for researchers, the data for health research come:

- from the participants themselves, *and/or*
- from providers.

They then go to a:

- research institute

³³ In the definition of processing (Article 4 paragraph 2 GDPR) and in the definition of 'recipient' ('whether or not a third party to whom personal data are disclosed', Article 4 paragraph 9 GDPR).

³⁴ Government Gazette 2004, no. 82.

³⁵ Article 7:457 of the Civil Code.

Although the standards are primarily aimed at researchers, those responsible for processing must ensure that they are also implemented and facilitate their implementation. In the Code of Conduct, the controller of the study is called the 'research institute'. This is a term that corresponds to Article 44 UAVG and Article 41 of the CBS Act.

Incidentally, Dutch legislation does not provide clarity as to what may be regarded as a 'research institute'.³⁶ The Code of Conduct assumes that this choice is deliberate. If only those who have been appointed by or pursuant to law may be designated as research institutes, the state would determine who may conduct scientific research and therefore health research in the sense of the Code of Conduct. Needless to say, this quickly leads to an extremely uncomfortable situation. Conflict with the principle of freedom of research³⁷ enshrined in the EU Charter would then be obvious. This does not alter the fact that legislation can designate organisations whose explicit task it is partly to conduct health research and which also receive funding for this purpose. This applies to UMCs³⁸ and Municipal Health Centres, for example.³⁹ But there are also a very large number of foundations that conduct scientific research⁴⁰ alongside commercial enterprises. The Code of Conduct and the research exemptions⁴¹ apply to all of them, including those mentioned in Article 44 UAVG.

The limitation lies in the way scientific research is conducted. It must comply with this Code of Conduct and therefore also with the standards of scientific integrity incorporated in it, in addition to the standards of responsible methodology and data protection included in it. This ensures that whatever the background of the organisation, the research must be conducted with integrity in order to fall under the Code of Conduct.

Previously, the term research institution was used. This raises the question of whether a natural person can also be the data controller for health research. In general, the Code of Conduct considers it unlikely that an individual who is not an employee of an institution can meet the conditions of the Code of Conduct in health research.⁴² See for example section 2 on strict data security standards. An exemption

³⁶ The concept of an institution for scientific research is not defined in either Act. The CBS Act refers in Article 41 (2) under b to an organisation or institution for scientific research established by law, but in paragraph e it also mentions research departments of other institutions. The Explanatory Memorandum to the UAVG or to the former Personal Data Protection Act (Parliamentary Papers 25892, no.3), from which Article 44 UAVG was largely taken, does not provide a starting point to further define what does and does not qualify as an institution for scientific research.

³⁷ Article 13 Charter of Fundamental Rights of the European Union.

³⁸ Article 1.4. Wet op het hoger onderwijs en wetenschappelijk onderzoek (Law on Higher Education and Scientific Research).

³⁹ Article 14 Public Health Act.

⁴⁰ Often with public subsidies, by the way

⁴¹ Compare also the broad definition of scientific research in Recital 159 GDPR.

⁴² For other types of research such as normative research, this is of course different.

is sometimes made for the physician-investigator who is not employed by a healthcare provider. As argued in chapter 10, in that case the healthcare provider will usually be jointly responsible for processing the data in order to guarantee the norms of data security and coding.

A person responsible for processing personal data for the purpose of scientific research is therefore a research institute in the sense of the Code of Conduct. It is quite possible that the person responsible for processing has other processing activities and tasks besides being a research institute. This is explained for UMCs in the section directed at researchers.

When drawing up the Code of Conduct, it proved possible to explain the legally correct but difficult distinction between 'provider' (can be an individual care provider or a data controller) and research institute (always a data controller) and the concurrence (within a research institute, payments for scientific research can also be made by individual care providers) sufficiently clearly in the reader's guide. The researchers found this difficult but not insurmountable.

- Care provider

This term is not mentioned in the Guide but does occur a number of times in the Code of Conduct. This term is in line with the Healthcare (Quality, Complaints and Disputes) Act.⁴³ The Act on Additional Provisions for Processing Personal Data in Healthcare is also in line with this concept.⁴⁴ In order to be able to act as a provider in health research, the controller to which the care provider is affiliated must implement a number of standards from this Code of Conduct. This could become part of the healthcare provider's information management and security system, or at least be in line with it. The healthcare provider must always have implemented such an information management and security system.⁴⁵ Therefore, this also falls outside the scope of this Code of Conduct.

- Legal basis

With regard to legal bases, on which the research institute must be able to rely, the legal finesse has been left out that only Article 6.1 GDPR formally provides a basis and Article 9.2 GDPR and EU or national legislation based thereon, the exemption to a prohibition on processing special category data. In this Code of Conduct both are referred to as a basis. As health research will always involve special category data at some point, both 'grounds' will usually have to be met.

⁴³ Article 1.1 Wkkgz.

⁴⁴ Article 1c Wabvpz.

⁴⁵ See the Decree on Electronic Data Processing by Healthcare Providers.

1 Research design

This chapter describes what should be considered when designing health research from a data protection perspective.

The chapter covers a number of important principles of the GDPR in health research, in particular Articles 5.1 and 89.1 GDPR. It elaborates on Article 25 GDPR, like the next one, and the attention of researchers is drawn to Articles 30 and 35 GDPR. Article 30 GDPR is further specified for data controllers in the context of health research.

The chapter also elaborates on the duty of data controllers to demonstrate that data processing is carried out in accordance with the GDPR, a duty which follows from Article 24 GDPR. The research protocol described in this chapter justifies the data processing for research purposes, initially by the researcher and therefore also by the data controller.

One of the purposes of the GDPR for data processing in the context of scientific research is to achieve a balance between data protection and scientific research, provided it is allowed to bear that name. The balance must therefore take into account the methodological principles for sound scientific research, namely that in the terms of this Code of Conduct, it also fulfils the conditions for scientific integrity according to the Dutch Code of Conduct for Scientific Integrity. Such research must therefore also meet the conditions for a responsible methodology.⁴⁶ A balance must be struck between responsible methodology and the conditions for data protection.

1.1 Research protocol and data management plan

This chapter essentially describes how researchers should think ahead about why they are doing what they can and are allowed to do with which data. A research protocol and data management plan serve this purpose.

The research protocol and data management plan (DMP) play an important role in the accountability and transparency of research under the GDPR. Both ensure transparency and accountability about the research and the considerations involved under the GDPR and in the context of this Code of Conduct.

⁴⁶ See for a description of the methodological principles of health research, for example: Bouter, Dongen & Zielhuis 2005; Many of the principles of good health research can be found as norms for good research practice in the Dutch Code of Conduct for Scientific integrity 2018 and further expanded on in Swaen e.a., *Journal of Clinical Epidemiology* 2018/100.

A research protocol is not required by the GDPR but is generally good practice in health research. For example, it is an essential link in the assessment of health research (section 1.3). Here it also forms a link with the general principles of the GDPR (Article 5.1) and subsequent provisions (Articles 24, 25 and 89.1). Much of that justification, for example about the foundations, is covered later in the Code of Conduct. This chapter can be seen as a rough roadmap of the other terms dealt with in the Code of Conduct.

The legitimacy of processing also depends on following the scientific rules of the art in terms of methodology and design. Otherwise, the standards of scientific integrity cannot be met.

The draft's interpretation of principles such as data minimisation and data protection by design and default has this dual purpose:

- comply with the GDPR; *and*
- meet methodological requirements for health research.

'Big data' research and/or research that does not test a hypothesis (i.e. without a clearly defined prior research question) is not excluded, provided that it can be methodologically justified (and provided, of course, that the other conditions of the Code of Conduct are met). 'Data minimisation' (Article 5.1.c GDPR) is not a goal in itself. The provision states that the data "must be limited to the purposes for which they (the data) are processed". The purposes in big data research are different from those in hypothesis-driven research. The researcher must be able to justify this in the research protocol.

The standards make it clear that also in the case of big data research, the protocol must always provide an overall description of the intended purposes of the processing, for example the hypotheses or insights that are expected to be gained, and must also provide a justification of why these data and data sources are needed, and how data minimisation will be carried out in the chain of data processing for the research in view of these purposes (chapter 2). This may apply, for example, to the development of decision models through AI (artificial intelligence) and to the special acquisition of data and human tissue for future scientific research (such as inclusion in a database or biobank). For the latter, see also chapter 4, in particular section 4.4.

1.2 Anticipating follow-up activities for data protection

The norm described here states that the researcher must think ahead and refers in the explanation to the other standards which, in connection with the layered structure of the Code of Conduct, will be discussed later. This norm requires no legal explanation.

1.3 Review, notification and implementation of data protection impact assessment (DPIA)

Section 1.4 is also included in this explanatory memorandum. These sections deal with two typical GDPR topics and one that is not.

The typical GDPR subjects are the register and the DPIA. The Code of Conduct thus implements Articles 30 and 35 GDPR. Formulating these standards at the level of the researcher is an important contribution to ensuring compliance with the GDPR by those responsible for processing. Norm 1.4.2 further contributes to the register being able to fulfil its data protection function.

The standards on DPIA are aligned with the criteria of the EDPB and AP.

The GDPR does not require a prior review or assessment of health research, but the Code of Conduct does, in principle. Assessment of health research is an important safeguard to ensure that the design and intended conduct of the research comply with this Code of Conduct. It is therefore an additional safeguard. Except for research that is subject to the WMO, the Netherlands has no statutory regulations for the (ethics) review of health research. In the near future, under the WzI,⁴⁷ the review of the removal of human tissue for research and research with human tissue will be added. Review or assessment of health research not covered by these frameworks also takes place, for example in a review procedure or by a privacy committee. It should be noted in passing that the review and assessment of research involve a great deal of regulatory pressure, with much research being reviewed several times and sometimes in contradictory ways.⁴⁸ For this reason, section 1.4 of the Code of Conduct also provides a number of indications for streamlining assessment and review procedures. In addition, the Code of Conduct will result in less divergent judgements.

⁴⁷ Bill on the Control of Human tissue.

⁴⁸ Boeckhout e.a. 2020; Van Agt, *Medisch Contact* 21 oktober 2020.

1.4 Responsibilities for institutions

The responsibilities mentioned follow directly from the previously discussed standards. They do not require any further legal justification here.

2 Appropriate safeguards

In a number of provisions, the GDPR or the UAVG leaves more room for [scientific research](#) than for other types of [processing](#), provided that so-called appropriate safeguards are in place (Article 89.1 GDPR). This means that technical and organisational measures must be taken which, among other things, give substance to the principle of [minimisationdata minimisation](#). This chapter describes the measures that must be taken in any case. This also implements the principle of '*data protection by design and default*' (Article 25 GDPR).

This chapter is an elaboration of, in particular, Articles 89.1, 5.1.b and c, 24 and 25 GDPR.⁴⁹ In this way the Code of Conduct ensures that these provisions are complied with in health research.

2.1 Data minimisation

This section provides an interpretation from the general GDPR principles mentioned above, in particular the GDPR principle of [data minimisation](#) data minimisation. This means that personal data must be 'adequate, relevant and limited to what is necessary for the purposes for which they are processed' (GDPR, Article 5.1.c). In the previous section it was already noted that, as the text of Article 5.1.c states, this does not mean 'absolutely as little as possible' but a balance between the methodology of the research and this GDPR principle. The elaboration offers researchers clear instructions for translating this principle of the GDPR into practice in health research. The elaboration is in line with general privacy design strategies.⁵⁰

2.2 Data protection when providing

The starting point is again the chain, from the provider to the researcher (research institution). This section primarily reflects Article 89.1 GDPR. In addition, Article 25 GDPR has also been incorporated into this section.

⁴⁹ A number of articles of the GDPR refer explicitly to Article 89.1 GDPR, particularly when those articles permit exceptions to general principles of the GDPR for scientific research. Incidentally, the text of Article 89.1 GDPR shows that it also has independent meaning for any scientific research.

⁵⁰ Hoepman, J.-H. 2018.

The following needs to be explained. As in the definitions, the section makes a distinction between one-way coded data and pseudonymised data. Coding is the umbrella term. It includes one-way coding and pseudonymising. With one-way coded data, there is no 'key' back to the data (usually directly identifying) on which the code number is based. One-way coded data are therefore not pseudonymised data within the meaning of the GDPR.⁵¹ For pseudonymised data, please refer to the definition in Article 4.5 GDPR.

The Code of Conduct does not provide further guidelines as to when data is or is not anonymous. That is always context-dependent. The code of conduct does refer elsewhere to 'statistical disclosure control' techniques when anonymous data are published as 'open data'.⁵² It has been suggested in the literature that another standard might apply when data are processed in a strictly secure environment (where export of the research data is not possible).⁵³ These proposals are partly based on the Breyer judgment,⁵⁴ which sets a different, more context-specific standard for anonymous data than Opinion 5/2014 of the former Article 29 Working Party. The EDPB has not yet explicitly commented on the relationship between the Breyer judgment and Opinion 5/2014. The relatively open-ended nature of the Code of Conduct in this area does not prevent the Code from being adopted. It just does not anticipate a discussion that does not yet appear to have been concluded.

Incidentally, section 2.2 contains practical guidelines for researchers on which form of coding is appropriate and when. This is a sufficient explanation/specification of the GDPR in this regard.

In addition, the section contains a specification that is of particular importance in connection with the rights of participants. Those rights include more than data protection. For example, it must be possible to feedback findings when appropriate. This means that some form of coding may be necessary, namely pseudonymisation, even though, from a data protection point of view, one-way coding may be preferable.

⁵¹ Compare the definition in Article 4.5 GDPR. This provision states that there are additional data that can be used to link the personal data to a specific data subject. With more advanced pseudonymisation techniques, this is the key in the sense of a two-way hash. In less advanced techniques, it is a simple cipher list. Mrs X becomes number 123, etc. Incidentally, it is questionable whether such a list satisfies the other condition of Article 4.5 GDPR, namely that the list must not only be kept separate in this case, but also that there are sufficient technical and organisational conditions to keep the list secret.

Incidentally, the definition often seems to be misread. Namely in the sense of: 'because data are pseudonymised, they are personal data'. But the definition starts with the fact that it is already personal data, whereupon an additional safeguard is put in place. Nevertheless, the Code of Conduct assumes that when there is a 'key' back, it is personal data.

⁵² See norm 12.9.1 where it refers to: <https://repository.wodc.nl/handle/20.500.12832/3057>.

⁵³ Groos & Veen, *European Data Protection Law Review* 2020/6 en de daar aangehaalde literatuur.

⁵⁴ HvJ EU 19 oktober 2016, ECLI:EU:C:2016:779 (*Breyer, C-582/14*).

2.3 Prohibition on reidentification

The significance of the ban on reidentification is obvious. Research institutions should implement this prohibition in employment and confidentiality agreements and/or institutional policies. A clause against violation of this prohibition is already standard in most *data-sharing agreements*, and it is also sanctioned against through data protection supervision (section 11.2). Under certain circumstances, violation could lead to dismissal.⁵⁵

2.4 Handling of directly identifying personal data

This section specifies the application of Articles 89.1, 24 and 25 GDPR to health research. See also chapter 8 for the retention period of research data. Article 25 GDPR is further elaborated for health research by setting standards for access. Only in exceptional cases will the researcher have access to the directly identifying data of the participants. These exemptions are described in sufficient detail in the Code of Conduct to meet the aforementioned provisions of the GDPR.

2.5 Access Security

This section specifies the application of Articles 89.1, 24 and 25 GDPR to health research. See also chapter 8 for the retention period of research data.

⁵⁵ For the situation of unlawful access to patient data, see for example: District Court Amsterdam 6 February 2018, ECLI:NL:GHAMS:2018:409.

2.6 Responsibilities for institutions

This section elaborates the standards for data controllers. The bar is set high by referring to a number of ISO or NEN standards. Healthcare providers often already implement these standards. It is possible to link up to them.⁵⁶

⁵⁶ If the research institution is also a healthcare provider, it must already comply with the Decree on Electronic Data Processing by Healthcare Providers, currently based on Article 9.2.1. [Section 15j, subsection 1, of the Act on Additional Provisions for Processing Personal Data in Healthcare.](#)

3 Informing data subjects

This chapter deals with the obligation to inform participants and is an elaboration of Articles 13 and 14 GDPR and the EDPB Directive on transparency.⁵⁷ Transparency is a necessary but not sufficient legitimation to process personal data. In addition, there must be a '[basis](#)', for example. Bases will be discussed in the next two chapters. In doing so, we will refer back to what has been discussed in this chapter. The explanation in the introduction makes it clear that the general privacy statement and the specific research information are communicating vessels, as it were.

3.1 Informing data subjects about data processing

This section contains the elements about which data subjects must be informed on the basis of Articles 13 and 14 GDPR. Legally, this speaks for itself. In practice, however, it will often be difficult to achieve a good balance between completeness and simplicity of language, etc. Partly for this reason, the Code of Conduct advises offering the information in layers, in line with the EDPB.⁵⁸

3.2 Exemptions to the principle of information provision by the research institution

Section 3.2 deals with the exemptions to the obligation to provide information. The exemption under a in Article 3.2.1 follows from Article 11 GDPR. In the case of coded data, the research institute does not have access to communication data. It is therefore practically impossible to inform every participant personally. Chapter 6 deals with the situation when the participant still provides additional information so that he/she can be uniquely identified. That is a different situation from the one at issue here, namely the question of when the research institute should directly inform the participants about the data processing of its own accord.

The remainder implements the exemptions for scientific research in Article 14.5 GDPR. Part b of Article 14.5 GDPR is elaborated in part c of norm 3.2.1. The drafters of the Code of Conduct consider the assessment framework for data processing on the basis of no objection referred to in this norm to be

⁵⁷ *Guidelines on Transparency under Regulation 2016/679 (wp260rev.01)*.

⁵⁸ *Guidelines on Transparency under Regulation 2016/679 (wp260rev.01)/35, 36*.

an adequate translation of Recital 62 GDPR and the remarks made earlier by the Article 29 Working Party.⁵⁹ Part d of Article 14.5 GDPR is not considered relevant in the context of health research.

3.3 Information and control of disclosure for secondary use: provider responsibilities

Section 3.3 is a specific elaboration of the provisions of Article 13.1 under c, d and e of the GDPR for health research. The purposes of the data processing and the recipients may thus not surprise a data subject.⁶⁰ Chapter 5 in particular builds on this.

⁵⁹ *Guidelines on Transparency under Regulation 2016/679 (wp260rev.01)/61.*

⁶⁰ *Guidelines on Transparency under Regulation 2016/679 (wp260rev.01)/45.*

4 Conditions for research involving the collection of new data and human tissue from participants

This chapter deals with the principles of processing data collected from participants specifically for research purposes. For this purpose, those participants must first have been invited and have given their consent. This chapter therefore deals with the conditions under which participants can be invited by other persons than the researcher and specifically with the conditions for such consent.

A number of principles apply to the processing of personal data. In addition to those discussed in the previous chapters, there must always be a legitimate [basis](#).⁶¹ In addition, there must be a legitimate ground to break the ban on processing [special category data](#).⁶² Although not strictly dogmatically correct, this is also called a basis here.

This chapter therefore particularly secures the provisions of Articles 6 and 9 GDPR and, because consent is almost always the basis for processing personal data obtained from the participants themselves, also Article 7 GDPR in conjunction with Article 4.11 GDPR. The provisions on consent for the processing of human tissue in research in the WzI (particularly Section 14 WzI) are in line with this. The sections of the WzI will not be referred to again below for the sake of readability and because the bill had not yet been adopted when this Code of Conduct was completed. In connection with this, the provisions of Article 13 GDPR are touched upon. Article 13 GDPR has already been elaborated on in chapter 3 of Part 1.

The request for consent is preceded by the processing of personal data in order to be able to invite potential participants. Article 5.1.b last sentence of the GDPR is important in this respect. In this phase other grounds than Articles 6.1.a and 9.2.a GDPR are also relevant for research institutions. This will be dealt with in the next section.

4.1 Approaching potential participants

This section deals with how a potential participant can be approached and invited to participate in a research study, thus implementing Articles 5.1b, 6.1e and f GDPR as possible grounds, and the interim EDPS opinion on data protection and scientific research.

⁶¹ Article 6 GDPR.

⁶² Article 9 GDPR.

Two phases of data processing must be distinguished:

- At the organisation processing the personal data to invite or possibly to provide to the research institution.
- At the research institution to process the personal data received to initiate the invitation and request for consent.

The latter aspect is the least problematic. There is no question of special category data (see below that the research institute never receives these at this stage). For the research institute, the basis will then be Article 6.1.e GDPR ('necessary for the performance of a task carried out in the public interest') or Article 6.1.f GDPR ('necessary for protecting the legitimate interests of the controller or of a third party'), depending on the legal status of the research institute.⁶³ In the Netherlands there are a large number of foundations that conduct scientific research in healthcare, such as the NIVEL, the Trimbos Institute and the IKNL. Even though the vast majority of this research is carried out with government funding, they are subject to Article 6.1.f. In view of the safeguards described in the Code of Conduct, it cannot be said that in this case, inviting the data subject to participate in health research outweighs his fundamental rights and freedoms.

Further distinctions are made at the first stage. Under the WBRP,⁶⁴ the controller can make a selection of the personal data of those registered, and this selection can be provided to a research institute. In that case the processing to select and supply is based on the law.

In other cases, there are two steps.

The first step is always that the controller makes a selection. Hardly anyone whose personal data is processed by the data controller will be invited to participate in the study. It will involve a certain selection, such as within a certain age range or other characteristics. Selection is further processing of personal data. The original purpose is not health research, but processing for the purpose of, for example, personnel administration or patient treatment. This further processing is acceptable on the grounds of the second part of Article 5.1.b GDPR which states that further processing for scientific research and statistics is not incompatible with the original purpose. Article 6.4 GDPR is not applicable

⁶³ If, for example, it is the RIVM or a UMC, 6.1.e. See Article 3 of the RIVM Act and Article 1.4 paragraph 1 of the Higher Education and Research Act, respectively.

⁶⁴ Article 3.16 BRP.

then.⁶⁵ The authors of the Code of Conduct are aware of the fact that the EDPS, in his preliminary opinion on scientific research and the GDPR,⁶⁶ had reservations about a possibly too broad application of Article 5.1.b GDPR. However, the fact that this should lead to the application of the test of Article 6.4 GDPR is contrary to the construction of the GDPR and Recital 50. The restriction must lie in the nature of the research. In this respect, the Code of Conduct meets the concerns of the EDPS. It should in the first place be about (approved) health research respecting principles of research integrity. This follows from the earlier provisions of the Code of Conduct. The next limitation is that the secondary use for the purpose of scientific research pursuant to Article 5.1.b is only applicable to the data controller who already processes⁶⁷ the data on a certain basis and then only by those who, based on their role in the data processing, already had access to those data. In the case of care providers, the circle is narrowed further.⁶⁸

Providing personal data to the research institute can also take place on the basis of Article 5.1.b, last sentence. The research institute is then a recipient, and the privacy statement (see the previous chapter) must provide for this. In practice, this will not happen often. In that case, the data controller must act as described below.

For receiving and therefore processing special category data, the research institute will need to have an additional ground based on Article 9.2 GDPR and any European and national legislation. Unless there is a situation as described in chapter 5, this is not the case at this stage. If the data originates from a healthcare provider, then this is special category data, especially if a selection has been made.⁶⁹

In this case, the original data controller must send the invitation from the research institute. The Code of Conduct describes in broad terms how this is often done, namely through the engagement of a processor on behalf of the data controller who processes the personal data for the original purpose.

⁶⁵ See also Recital 50 GDPR which explicitly mentions the compatibility for scientific research and statistics in the explanation of this provision.

⁶⁶ European Data Protection Supervisor 2020.

⁶⁷ For healthcare providers, this is Article 6.1.c GDPR (keeping records is required on the grounds of the WGBO) in conjunction with 9.2.h of the GDPR/ Article 30 UAVG.

⁶⁸ The submitters are aware that the EDPB in their answers to questions from the commission suggested that the second clause of article 5.1. GDPR does not apply to special personal data. That notion is not expanded on. Without a convincing argument why especially this part of article 5 doesn't apply to special personal data while the rest of the article does (since it follows from the flow of the GDPR, the general principles apply all the way through), this suggestion is ignored. European Data Protection Board (EDPB) 2021.

⁶⁹ In theory, an exception could be made for data from a GP if the selection is made solely on the basis of general characteristics such as age or gender. Being registered with a GP says nothing about health. Almost every resident is registered. In order not to make it too complex, the code of conduct ignores this nuance.

4.2 Express prior consent to data processing

If consent in the sense of the GDPR is the basis, this and the following sections determine what that consent must satisfy. The Code of Conduct assumes that GDPR consent is always the basis - barring a statutory exemption - if the data for the research is collected directly from or via the participants. This chapter of the Code of Conduct thus implements Articles 4.11, 6.1a, 7, 9.2a GDPR, Recital 43 GDPR and the EDPB guideline on consent.⁷⁰

The use of the term 'GDPR consent' has been chosen in order to distinguish it in the first place from consent for participation in research that is subject to the WMO, but also to avoid confusion with the term 'general consent' introduced in chapter 5.

Consent within the meaning of the GDPR is strictly defined; it must be freely given, specific, informed and an unambiguous expression of will. These elements mean that for a set of processing purposes, GDPR consent must be granular⁷¹, which means that consent can never be given for a set of processing purposes but must always be given separately for different processing of personal data. This granularity is expressed first and foremost in norm 4.4.3 on research with special privacy risks or consequences. If such consequences may be involved, the consent must specifically relate to them.

Although the EDPB emphasises that besides consent there are also other grounds for scientific research,⁷² the Code of Conduct assumes that when data are collected directly from the participant, explicit consent in the sense of Article 4.11 in conjunction with Article 7 of the GDPR must always be the basis under Dutch law. This is not only fairer vis-à-vis the potential participants, under Dutch law there is no other basis when approaching the participant to obtain new data for scientific research.

Only the data processing for clinical trials with medicinal products has a different basis, namely the European laws and regulations concerning this trial,⁷³ or at least the trial conducted on the basis of the

⁷⁰ European Data Protection Board 2020.

⁷¹ European Data Protection Board 2020, p. 12. Zie ook Overweging 43 GDPR.

⁷² European Data Protection Board 2020, p. 5. European law does have a different basis in one situation, namely the regulation of clinical trials involving medicines.

⁷³ Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials of medicinal products for human use; Commission Delegated Regulation (EU) 2017/1569 of 23 May 2017 supplementing Regulation (EU) No 536/2014 of the European Parliament and of the Council by specifying principles of and guidelines for good manufacturing practice for researching medicinal products for human use and arrangements for access; Commission Implementing Regulation (EU) 2017/556 of 24 March 2017 on the detailed arrangements for the good clinical practice access procedures pursuant to Regulation (EU) No 536/2014 of the European Parliament and of the Council.

approved protocol. This does not alter the fact that the potential test subject must be informed of the data processing. The provisions of chapter 3 remain applicable. Consent to participate in the trial therefore also includes consent to the data processing inherent in it. However, for data processing outside the trial protocol, for example for re-use, the provisions on an GDPR basis apply in full.

With the exception of the legally regulated situations of new data collection in the case of research or human tissue that is subject to the Medical Research (Human Subjects) Act (WzI), the code of conduct does not address other health research in emergency situations. As the data must be obtained from the participants themselves, this will probably not be the case outside of the aforementioned statutory situations. Health research will then fall under secondary use to which the provisions in the next chapter apply.

In 4.2.2 the Code of Conduct deals with the representation of young persons under 16 years of age and groups subject to a special protection order. If a legal representative gives consent, the same basis applies as if the data subject had given consent.

Furthermore, the Code of Conduct follows the legal provisions.

Pursuant to Article 5.1 UAVG, minors under the age of 16 are represented by their legal representative.⁷⁴ According to Article 5.2 UAVG, the same applies to data subjects who have been placed under guardianship or for whom an administration or mentorship has been established. For the group mentioned in Article 5.2, the UAVG states that this only concerns matters for which the data subject is incompetent or unauthorised. The Code of Conduct assumes that, with the exception of research under the WMO Act, persons under guardianship must be able to speak for themselves and that participation in health research is not a matter for which the person involved is incompetent or unauthorised.

Pursuant to Article 7:465.1 of the Dutch Civil Code, the obligations of the counsellor towards the patient are directed towards the parents of the patient if the latter has not yet reached the age of 12. It follows that the child from the age of 12 has an independent right to confidentiality of his data. It follows from Article 7:450.2 of the Dutch Civil Code that patients who have reached the age of 12 but are not yet 16 also require the consent of the parents who exercise authority over them or are their guardians (double consent). The same requirement of double consent follows from Article 6.b WMO.

⁷⁴ According to Article 8 GDPR, national legislation may set a lower age, but not lower than 13 years. This is not the case in the Netherlands, unless it concerns 'assistance and counselling services offered directly and free of charge to a minor' (see Article 5.5 UAVG).

4.3 Informed consent

This section relates to the requirement that GDPR consent must always be informed, and elaborates on Articles 4.11 and 13 GDPR, and the EDPB Guidelines on Consent⁷⁵ and Transparency.⁷⁶

The enumeration in 4.3.3 with which participant information must comply is taken from Articles 13.1 and 13.2 GDPR, insofar as relevant. Points g and i of norm 4.3.3 do not appear in Article 13 GDPR and were added by the authors of the Code of Conduct. For a further explanation of these elements, see the justification in section 4.4 (about research and applications with special risks and consequences for the participant).

4.4 Specific authorisation

This section deals with the specificity requirement of GDPR consent, and elaborates on Article 4.11 GDPR and the EDPB Directive on consent.⁷⁷

The specificity requirement is reflected in the fact that, in addition to the purposes of the research, participants should also be informed about:

- special privacy risks or consequences;
- intended data linkage; *and*
- the possibility of re-using data for new, future research.

The particular privacy risks or consequences of the above elements will be explained.

Research with special privacy risks or consequences is not mentioned as such in the GDPR⁷⁸ or EDPB guidelines. Special privacy risks or consequences include 'sensitive applications' from the draft WzI bill

⁷⁵ European Data Protection Board 2020, p. 15.

⁷⁶ *Guidelines on Transparency under Regulation 2016/679 (wp260rev.01)*.

⁷⁷ European Data Protection Board 2020, p. 13–14.

⁷⁸ The GDPR does refer to processing operations with a 'high risk to the rights and freedoms of natural persons' in Recital 94, but the concept of 'special privacy risks or consequences' is broader.

but have a broader scope. The term was introduced in the Code of Conduct to make the point that certain research is extra sensitive.

Research with special privacy risks or consequences relates to research that either does not fall within the reasonable expectations that people generally have of scientific research in healthcare or that can have consequences specifically for the participant. In the case of the first type of research, cooperation with a commercial party may be considered, whereby the benefits may also accrue to that party. For example, the use of human tissue to form organoids also falls outside the current reasonable expectations.

Consequences for the participant include situations in which it is foreseeable that the intermediate stage between publication of the results of the research and their application in practice or in policy, which is usual in health research, will be interrupted. Certain findings have immediate consequences for certain participants without that intermediate stage. The most obvious example is findings that may have direct consequences for the future health of the participant or his/her relatives. There may also be other examples, particularly where patients are involved in research into 'personalised medicine' for their condition. Results will then be fed back directly to the patients involved. The participant should be aware that he or she may be confronted with the results of the research in a very direct manner. Incidentally, before these results are applied in the treatment, an informed consent procedure in the sense of the Wgbo will be carried out.⁷⁹ This falls outside the scope of the code of conduct.

The participants must always be explicitly informed about these forms of research and the possible risks and consequences involved and must give their separate consent. The Code of Conduct thus offers an additional guarantee for the protection of the rights and freedoms of those involved.

The category of research with special privacy risks or consequences is reflected in a number of places in this Code of Conduct. See below in the next section and the next chapter.

⁷⁹ Article 7:450 of the Dutch Civil Code

4.5 Further specification of consent in the case of wide-ranging research

This section deals with the specificity of consent in long-term, wide-ranging research. In principle, GDPR consent should be as specific as possible. Recital 33 of the GDPR⁸⁰ recognises that it is not always possible to fully describe the purpose of the data processing for scientific research at the time of collecting the personal data. In this case, consent may be given for certain areas of scientific research, provided that it is in accordance with the standards of scientific integrity.

This consideration also seems to offer scope for broad consent, as is the case in a large number of Dutch long-term cohort studies.⁸¹ Internationally,⁸² this is also customary for much scientific research.⁸³ However, the EDPB gives a restrictive interpretation of Recital 33⁸⁴ and emphasises that the Recital cannot be used as a licence to 'circumvent' the specification of the purposes.

When the research purposes cannot initially be sufficiently specified, the EDPB states that the controller must find other ways to ensure the spirit of the consent requirements.⁸⁵ The EDPB makes a number of suggestions for this, including dynamic consent and dynamic opt-out.⁸⁶

The Code of Conduct provides a balance between the strict approach of the EDPB and the existing consensus on broad consent. Under a number of conditions, it is also possible to request broad consent from participants. In essence, these come down to the following:

1. The participants are appropriately informed about the sub-studies that are carried out with their data and human tissue within the broad objectives;
2. If sub-studies with special privacy risks or consequences are set up, separate consent must always be requested;
3. It is checked whether the course of the study still corresponds to the reasonable expectations of the participant;
4. If this is not the case, the participant will be asked for consent again.

⁸⁰ The recital reads: 'It is often not possible at the time of collecting personal data to fully determine the purpose of the data processing for scientific research purposes. Therefore, data subjects should be allowed to give their consent for certain areas of scientific research in compliance with recognised ethical standards for scientific research. Data subjects should be given the opportunity to give their consent only for certain areas of research or parts of research projects, to the extent that the intended purpose allows.'

⁸¹ For example, [Lifelines](#), [Generation R](#), [Twin Register](#) and [Amigo](#).

⁸² For example, the [UK Biobank](#).

⁸³ Hallinan, *Life Sciences, Society and Policy* 2020/16.

⁸⁴ European Data Protection Board 2020/155-157.

⁸⁵ European Data Protection Board 2020/159.

⁸⁶ European Data Protection Board 2020/161.

In the event of special privacy risks or consequences or partial studies that no longer reasonably match expectations, consent will have to be requested again. It is important that what is stated here applies in conjunction with other provisions in the Code of Conduct. This applies to everything in the Code of Conduct: the provisions of a specific section must be read in conjunction with the other provisions. In other words, the 'broad consent' is embedded in a system of data protection and integrity of scientific research. The authors claim that Article 7 GDPR in conjunction with Recital 33 is thus fulfilled. This strikes a balance between the importance of responsible health research, which would be impossible without a form of broad consent, and the requirements of data protection. Any more restrictive view would be contrary to the aforementioned balance that the EU legislator intended to achieve by including Recital 33 in the final version of the GDPR.

4.6 Freely granted consent

This section relates to the requirement that GDPR consent must always be freely given, and elaborates on Articles 4.11 and 7.4 GDPR and the EDPB Directive on consent.⁸⁷

The EDPB Directive gives a number of examples of situations in which consent may be involuntary. There may be an imbalance of power between the data subject and the controller,⁸⁸ the failure to give consent may have potentially adverse consequences for the data subject,⁸⁹ or the data subject does not have the option to give or withhold consent for separate data processing operations⁹⁰ (lack of granularity).

With respect to the freedom to consent, the Code of Conduct is in line with a long tradition in health law and medical ethics on informed consent for scientific research. A treatment relationship does not rule out asking consent to participate in scientific research, but depending on the type of research for which consent is asked, other safeguards may be applicable, such as a reflection period included in the WMO and the option of consulting an independent care provider. In keeping with the tradition mentioned above, the explanatory memorandum also calls for attention to be paid to preventing the 'therapeutic fallacy'. This doctrine means that participants may be under the mistaken impression that

⁸⁷ European Data Protection Board 2020, p. 7–13.

⁸⁸ European Data Protection Board 2020, p. 8.

⁸⁹ European Data Protection Board 2020, p. 10–12.

⁹⁰ European Data Protection Board 2020, p. 12.

they will derive personal benefit from participating in research.⁹¹ Proper provision of information during the research should prevent this. In addition, the explanatory memorandum mentions a number of other aspects which must be taken into consideration so that consent can indeed be freely given, and which are often already common practice.

4.7 Demonstrable consent

This section concerns the requirement of proof of GDPR consent and elaborates on Articles 4.11 and 7.1 GDPR, Recital 42 GDPR, Article 6 WMO and the EDPB Directive on consent.⁹²

As far as research subject to the WMO is concerned, it follows from Section 6 of the WMO that consent must be given in writing. An amendment of the law⁹³ currently in progress adds a second paragraph to this section, stating that consent may also be given electronically.

Recital 42 GDPR states that the burden of proof for consent always lies with the controller. The EDPB states that data controllers are free to develop methods to meet the requirement of proof in a way that fits into their daily operations.⁹⁴ However, a number of conditions must be met under this Code of Conduct: the identity of the participant must be reliably authenticated, the consent procedure must be documented, the responses must be reliably recorded, and verbal consent must be recorded according to a protocol.⁹⁵

4.8 Withdrawal of consent

This section concerns the withdrawal of consent and elaborates on Articles 4.11 and 7(3) GDPR. The explanation makes it clear that various situations of discontinuation of participation may apply.

Withdrawing consent for data processing must be distinguished from the situation in which a participant no longer wishes to actively participate in the research. This often happens in long-term cohorts and often appears indirectly, for example, because the participant no longer responds to a

⁹¹ 'Ethiek van medisch-wetenschappelijk onderzoek: informed consent en de therapeutische misconceptie | Nederlands Tijdschrift voor Geneeskunde', <https://www-ntvg-nl.eur.idm.oclc.org>.

⁹² European Data Protection Board 2020, p. 22.

⁹³ 2020–2021, 35 587, nr. 2.

⁹⁴ European Data Protection Board 2020/106.

⁹⁵ European Data Protection Board 2020/107-109.

new questionnaire.⁹⁶ Such discontinuation of participation is not a withdrawal of consent or an objection to data processing in the sense of the GDPR. If the participant no longer responds or replies that he or she no longer wishes to participate, the processing of the research data already collected can continue. The participant should not be approached again with new questionnaires.

This is different if the participant withdraws his or her consent within the meaning of Article 6.1a or Article 9.2a GDPR to the processing of his or her data. In that case, a different regime regulated by the GDPR comes into effect. Data or human tissue must be erased or destroyed in accordance with Article 17.1(b), unless one of the exemptions mentioned in the norm applies. These, in turn, give substance to exemptions to the right of erasure in Article 17.3 b-d GDPR. The elaboration does not go beyond what is necessary for the integrity of health research and is sufficiently defined and specific to serve as an adequate explanation/specification of the provision for a Code of Conduct.

⁹⁶ The 'retention problem' with long-running cohorts, as it is called in the English-language literature, has often been investigated, see for example: Teague e.a., *BMC Medical Research Methodology* 2018/18. That participants no longer take part does not mean they have withdrawn consent.

5 Conditions for secondary use

Chapter 5 discusses the grounds on which data and human tissue may be processed that have been collected for a purpose other than scientific research, 'secondary use'.

Specifically, the chapter deals with the situation that the data comes from healthcare. It incorporates the following standards from the applicable regulations:

- Articles 6.1, 7, 9.2 and 19 GDPR;
- Articles 24 and 28 UAVG; *and*
- Articles 7:457 and 7:458 of the Civil Code (WGBO).

The WzI is in line with the GDPR and UAVG as regards the interpretation of consent (in particular, Article 14 WzI) and exemptions to it (Article 17 WzI); these provisions are therefore also safeguarded. In addition, this chapter gives a further interpretation of Article 5.1.b GDPR. In that context, it was already discussed in the previous chapter (section 4.1) that secondary use for the purpose of health research by the person who has lawful access to the personal data that meets the conditions of the Code of Conduct is permitted on the grounds that further processing for the purpose of scientific research and statistics is, in principle, not incompatible with the original purposes of processing.

Own research by the care provider

The purpose limitation principle of Article 5.1.b GDPR and medical confidentiality of Article 7:457 of the Dutch Civil Code are not breached by so-called "own research" by healthcare providers. This is understood to mean a study conducted by a care provider using the data of a patient with whom the care provider has a direct treatment relationship and where the care provider is also authorised to inspect all data used for the research.

Legally, there is limited room for "own research" by care providers without meeting the standards discussed in this chapter (research based on consent or specific exemption). The research will then only be allowed to relate to patient data from the care provider's file. In the case of multidisciplinary treatment, this creates a great deal of ambiguity. Even then, such 'own research' will have to be limited to research with the data recorded by the care provider himself. Consent will always be required for any further analysis of the patient's human tissue.

"Own research" by healthcare providers without giving the patients concerned the opportunity to object or consent does not apply to healthcare providers who otherwise inform their patients about the research and ask them for consent or actively offer a possibility to object. In that case, it is ethically difficult to explain that this consent or option to object does not apply to one's 'own' healthcare provider (however demarcated).

5.1 Provision and secondary use of anonymous or anonymised data and human tissue

This section deals with the provision of anonymised personal data and elaborates on Article 5.1b GDPR, Recital 26 GDPR, Article 7:467 of the Civil Code and the WP29 opinion on anonymisation techniques.

97

Anonymising personal data counts as processing, which is why a basis is also required for this action. Anonymisation for the purpose of scientific research is in principle not incompatible with the original purposes of the processing (Article 5.1.b GDPR).⁹⁸ Access to the data for the purpose of anonymisation is restricted under this Code of Conduct (see section 5. 7). In addition, the Code of Conduct requires that anonymisation must take place for the purpose of scientific research as described in the Code of Conduct (see section 1 of chapter 4) or to comply with a legal obligation, for example to publish open data. Thus, the Code of Conduct contains sufficient guarantees to speak of compatible processing. Once data have been anonymised, they cannot be regarded as personal data, with the result that the GDPR no longer applies to them. Anonymous patient data also does not fall under the WGBO.⁹⁹ The authors of the Code of Conduct see no reason to extend a consent or objection system to the anonymisation of patient and other personal data, partly because the processing of such data no longer involves any risks for those whose data has been anonymised. Institutions are free to take previously expressed objections into account, even in the case of anonymous disclosures.

With human tissue, the situation is more complex. The WGBO contains a provision that anonymous human tissue may only be used if the patient has not objected (7:467 of the Civil Code). The distinction

⁹⁷ Article 29 Data Protection Working Party 2014.

⁹⁸ Article 29 Data Protection Working Party 2014/2.2.1.

⁹⁹ On this point the NFU deviates from its position. 'Handreiking Hergebruik van zorggegevens voor wetenschappelijk onderzoek 14-10-2020', p. 1, 4. The parliamentary documents of the WGBO do not provide any indication for this point of view. The discussion on the provision of data for the purpose of scientific research always concerned patient data that were still identifiable in one way or another. See also Parliamentary Papers 21561, no. 20, p. 3 at the top.

between anonymous and non-anonymous human tissue will lapse under the (draft) Wzl. Then consent will also be the main rule for anonymous human tissue, with the possibility of exemptions as discussed later in this chapter (sections 5.4-5.5).

5.2 Conditions for secondary use of special category data: consent as the starting point

Insofar as EU law or national law does not contain any exemptions,¹⁰⁰ the basis for the processing of patient data and human tissue for health research by a research institution is the explicit consent in the sense of the GDPR (Articles 6.1a and 9.2a GDPR and in due course Article 14 Wzl). Unless the researcher can request consent himself (see the previous chapter), such consent will have to be requested by the provider. This is the most common situation for secondary use as discussed in this chapter. The norm described in section 5.2 thus expresses Article 9.2.a GDPR and the national exemptions further elaborated in the chapter. The conditions of this GDPR consent were discussed in the previous chapter.

5.3 General consent for healthcare providers

Under certain circumstances, obtaining GDPR consent through the provider is either impossible for the research institution or requires a disproportionate effort.

A large number of healthcare providers structurally and regularly supply data and human tissue of patients to researchers/research institutions for secondary use in various forms of specific research. In these cases it is usually not clear beforehand which patients will have their data and human tissue supplied and for which research. To meet the conditions for GDPR consent, as discussed in the previous chapter, all these patients would at least have to be regularly contacted to inform them of the purpose for which their data or body tissue will be processed. This would require an extremely complicated ICT system at the healthcare provider, to be paid for by the research institution, and a plethora of e-mails or letters to the patients. If the patients have been out of treatment for some years, contact details may no longer be up to date, and this would also lead to more data breaches. Partly in view of the high threshold for obtaining specific consent in the sense of Article 9.2.a in conjunction with Articles 7 and

¹⁰⁰ Based on 9.2. i and j GDPR

4.11 GDPR, requesting GDPR consent is not really possible or costs a disproportionate amount of effort. The definition and norm of consent for supplying and processing human tissue in the Wzl are in line with this. The authors of the Code of Conduct argue that when patient data are systematically passed on to researchers, as is now the practice at many healthcare providers, a situation arises as described in Articles 24 and 28 UAVG (and Article 17 Wzl). They noted that the UAVG wanted to be as much in line as possible with the situation under the WBP.¹⁰¹ However, under the GDPR the threshold has been raised to be able to speak of explicit consent for data processing.¹⁰² And incidentally, it is now an EU law concept, not a concept determined under national law.¹⁰³ In order to perpetuate the situation under the WBP, it will therefore be necessary in more situations to ask for - thus now - GDPR (and Wzl) consent or to take a disproportionate effort than previously under the WBP.

In addition to the basis of Article 24 or 28 UAVG (and in due course Article 17 Wzl), the research institute will also need a basis in Article 6.1 GDPR. For this purpose, see section 4.2. In addition to the other provisions of the Code of Conduct, the guarantees laid down in this chapter ensure that the interests or fundamental rights and freedoms of the person involved do not outweigh the legitimate interest of the research institute in the case of Article 6.1.f GDPR. The guarantees in this chapter include the test that must precede the provision of data, the fact that the person involved must always be given the opportunity to give general consent or to object, and that only coded data may be provided.

Before researchers can lawfully process patient data or human tissue, care providers must have a legal basis for providing such data or human tissue to a third party. For data that are part of the medical file, this is regulated in Sections 7:457 and 4.458 of the Dutch Civil Code; for human tissue this can currently be concluded and will follow from the Wzl in due course. Here, too, consent is the main rule. However, this consent is not bound to the GDPR conditions of consent, but must be seen in the light of the establishment of the WGBO.¹⁰⁴ In GDPR terms, the WGBO falls under the exemptions to the consent referred to in Article 9.2.h but also contains elements of Articles 9.2.i and 9.2.j GDPR. Under the WGBO it is sufficient, under certain conditions, that general consent is given to provide patient data or human tissue to researchers.

¹⁰¹ For the UAVG, the legislator 'strived for a policy-neutral implementation of the Regulation in relation to the law in force under Directive 95/46/EC and the Personal Data Protection Act'. 2017, 34851, nr. 3.

¹⁰² Article 29 Data Protection Working Party 2018.

¹⁰³ See, inter alia, 34851, no. 3, pp. 104-105.

¹⁰⁴ Ploem, Rigter & Gevers, *Tijdschrift voor Gezondheidsrecht* 2020/44/2.3.

Those conditions are elaborated in this chapter. There is an accumulation of conditions. General consent cannot be unrestricted and must be related to the area or areas of the patient's illness. In the case of research with special (privacy) risks or consequences, GDPR (and/or WzI) consent must always be requested. In this way, the general consent, in conjunction with the other provisions regarding the provision of information and the privacy statement, can be in line with the reasonable expectations of patients.

This form of asking consent, in combination with the other safeguards provided in this Code of Conduct, is in line with the way in which the Dutch legislator has established consent as the starting point for secondary use. It simultaneously makes a number of things possible:

- Patients are personally informed of the possibility of secondary use and are given the opportunity to exercise control over this.
- Research is possible within the framework of the requested general consent. Providers and researchers are less dependent on separate consent procedures or on invoking the exemption to the principle of consent for each specific study.
- A simpler review and assessment of research and the question of whether data and human tissue can be provided. Discussion of the applicability of exemptions to the principle of consent in the sense of 7:458 of the Civil Code, Articles 24 and 28 UAVG (and Article 17 WzI) for specific research is unnecessary.

Healthcare providers that do provide regular information but are unable to organise general consent¹⁰⁵ are still obliged to inform patients personally about secondary use and to offer them a low-threshold opportunity to object.

By informing every patient and offering them about the possibility to object, a safety net is created for all research for which consent cannot be requested. In such situations, it will still have to be decided for each study whether or not GDPR consent can and must be requested from those who have not objected.

¹⁰⁵ The impossibility of organising general consent can be seen, for example, in the pilots that are currently running: despite the attempts to reach patients, there is such a non-response that de facto a large number of patients would fall under an objection regulation. The type of contact with the patient or client could also lead to the conclusion that, during the course of assistance or, for example, in the context of an appointment system, asking for general consent is impossible to organise.

A point for attention with general consent is that not every patient will be able or willing to respond immediately to the request for consent and possibly not every patient will be reached. Such patients must be given the opportunity at a later stage to give their consent or not. In the case of patients who do not respond, asking for consent in the sense of the WGBO also turns out to be impossible. In line with the 2004 COREON Code of Conduct on Health Examination, the current Code of Conduct provides an extra safeguard for such situations. Patients must be informed that if they do not respond, the care provider will assume that the patient does not object to health research using the patient data and/or human tissue.

A second possible consequence is that by asking for general consent, the patient will generally refuse while he or she would like to give consent for certain types of research. This could be a particular problem for national registries that aim to provide national coverage of at least the incidence and prevalence of the conditions, to be distinguished into various subtypes, covered by the registration. Unlike many other countries, the Netherlands has no legal regulation for such registries as the Dutch Cancer Registry (NKR). They also rely on the general no-objection system. In view of the numbers involved and the need for the most comprehensive coverage possible, asking consent is unreasonable. These circumstances are elaborated on in the next section. When introducing a general consent system, asking consent seems possible but could ignore the aforementioned specific circumstances of those registrations that are of great importance to public health policy.¹⁰⁶ The continuity of these registrations must be guaranteed. The code of conduct suggests that healthcare providers could build in a certain granularity to general consent, whereby such registrations would continue to fall under a no-objection system.

5.4 Exemptions to the principle of consent for special category data

Section 5.4 deals with the exemptions to the principle of consent for special category data. In a number of situations, it is not reasonably possible for the care provider to ask consent, or this cannot be reasonably expected. This section therefore elaborates on Section 7:458 of the Civil Code subsections 1 under a and b, by naming the concrete circumstances in which asking consent is not possible or cannot be required. This is in line with the parliamentary debate on the WGBO,¹⁰⁷ the COREON Code of Conduct for Health¹⁰⁸ Research approved by the CBP in 2004, and the legal and ethical consensus

¹⁰⁶ Coebergh e.a., *European Journal of Cancer* 2015/51.

¹⁰⁷ Parliamentary Papers 21561, no. 20, p. 3.

¹⁰⁸ Government Gazette 2004, no. 82

that has since been developed in the field to further flesh out the open standards of 7:458 of the Dutch Civil Code.¹⁰⁹ Research that meets these conditions also meets the exemptions to the principle of consent from the less strict regulation (according to the legislator) in Articles 24 and 28 UAVG (and Article 17 WzI).¹¹⁰ The basis in Article 6 GDPR has already been discussed above.

5.5 Conditions for secondary use on the basis of general consent or an exemption to the consent principle

Section 5.5 deals with the conditions that apply to secondary use based on general consent or one of the exemptions to the consent principle. The legal basis of the research institute is now at issue. In addition to the legal basis already discussed in Article 6.1 GDPR, this must be one that is based on Article 9.2 GDPR. The GDPR itself does not provide a basis for the processing of special category data for the purpose of scientific research without GDPR consent. The national exemptions are therefore at issue. This section primarily elaborates the cumulative conditions of both 7:458 of the Civil Code and Articles 24 and 28 UAVG (and Article 17 WzI).

For the description of the concept of 'public interest', one of the conditions from each of the aforementioned provisions, reference is made to the literature¹¹¹ and a Parliamentary Letter on secondary use.¹¹² The conditions from this Parliamentary Letter have also been adopted in the Explanatory Memorandum of the WzI.¹¹³

The text accompanying this section states in a footnote that the RIVM can sometimes invoke another national provision. For the RIVM, these provisions are, in particular, Article 6.c of the Public Health Act and Article 3.3 of the RIVM Act. These provisions were not mentioned in the basis for data provision (sections 5.2-5.4). These provisions are a basis for the RIVM to process data. They do not include an

¹⁰⁹ 'Handreiking Hergebruik van zorggegevens voor wetenschappelijk onderzoek 14-10-2020'.

¹¹⁰ For the regulation in Article 24 UAVG the legislator has 'partly' followed Article 7:458 of the Dutch Civil Code. The legislator indicates that the regulation of Article 24 UAVG is 'not as strict as that of the Civil Code'. See Parliamentary Papers 2017, 34851, nr. 3, p. 104-105.

¹¹¹ Commissie Regelgeving Onderzoek 2018.

¹¹² Ministerie van VWS, 'Kamerbrief met reactie op artikel over secundair gebruik data, 1587082-195476-DICIO', www.rijksoverheid.nl, doi:10/04/kamerbrief-over-reactie-artikel-fd-over-secundair-gebruik-data, 4 oktober 2019.

¹¹³ 2021, 35 844, nr. 3.

exemption to 7:457 of the Civil Code for the healthcare provider to provide information to the RIVM. This is still governed by the provisions of the previous sections.¹¹⁴

For the sake of completeness, it should be noted that other government bodies may also have a basis for processing special category data. Most relevant here are the CBS (Article 35 of the CBS Act), the Nederlandse Zorgautoriteit (Article 69.2 of the Health Care Market Regulation Act) and Zorginstituut Nederland (Article 68a of the Health Care Insurance Act). It would be going too far here to go into the bases and conditions for the compulsory provision of special category data to these bodies. The data, once obtained, may be used by these institutions for scientific research and statistics (see above under section 4.1). This is of course the first priority at the CBS (Section 3 of the CBS Act), and there are explicit rules about how other bodies than the CBS may use the data held by the CBS for scientific research (Sections 41-42a of the CBS Act).

5.6 Provider responsibilities: control of provision for secondary use

This section elaborates on the previous sections in terms of obligations for providers, particularly in the area of transparency about secondary use and the provision of an appropriate form of consent or an option to object that actually reaches the patients. This is the best way to implement Articles 13 GDPR and 7:457 and 7:458 of the Civil Code.

5.7 Provider responsibilities: institutional policy on secondary use

This section deals with a number of residual issues. Norms 5.7.1 and 5.7.2 express 7:457 Section 3 of the Civil Code. Access should be limited to those who are directly involved in the execution of the treatment agreement. The exemption in 5.7.3 was included in the 2004 Code of Conduct under the exemptions that asking consent is not reasonably possible. It is included here rather than in section 5.4 because it concerns a form of access and not the provision of data. Compared to 2004, the provision has been further clarified.

Incidentally, section 5.7 contains a number of standards which further secure the previous provisions regarding secondary use at the level of the data controller. In addition to the provisions in the final

¹¹⁴ In the case of infectious diseases that require reporting, the GGD must be informed. The GGD sends this information to the RIVM in pseudonymised form.

parts of 7:458 of the Dutch Civil Code subsections 1 and 2, norm 5.7.6 ensures that the rights of data subjects on the grounds of Articles 16 through 21 can be exercised as much as possible at the research institute. See the next chapter for more details.

The final section guarantees, in conjunction with what has been noted in chapters 1 and 2, among other things, that only those data are provided that are necessary for the research or the registration. This also ensures compliance with the provisions of Article 7:458 of the Dutch Civil Code and Article 24/28 UAVG (and Article 17 WzI), where applicable, that the research cannot be carried out without the data concerned.

6 Rights of participants with regard to data and human tissue

This chapter implements Articles 11, 14-22 GDPR and Article 44 UAVG.

Article 44 UAVG, which implements Article 89.2 GDPR, states that Articles 15, 16 and 19 GDPR may not apply to processing by institutions or services for scientific research purposes. In doing so, the necessary provisions must be made to ensure that personal data are processed solely for scientific and statistical purposes. This is ensured in particular in chapters 8 and 9. The legislative history (via the WBP) gives no indication of what (or who) may qualify as such institutions or services (see footnote 23 above). The Code of Conduct assumes that subscribing to the Code of Conduct provides sufficient guarantee that the data subjects in question may be regarded as scientific research institutions or services in the sense of the UAVG.

Article 44 suggests that the non-application can be done at the level of the research institute. The Code of Conduct takes a more restrictive approach, namely that it must be assessed for each research project whether the aforementioned provisions of the GDPR should not apply due to the nature of the research. This is in line with Article 89.2 GDPR, which leaves room for national exemptions to these rights 'insofar as those rights risk rendering impossible or seriously impeding the realisation of the specific purposes, and such exemptions are necessary to achieve those purposes'. This chapter provides criteria for assessing when this is the case. The criteria are also aligned with Article 17(3)(d) of the GDPR. This provision is further specified in this chapter.

According to the authors, the balance struck here satisfies the conditions to be imposed on a code of conduct by means of a proportional interpretation of the research exemptions and sufficient certainty/specification.

The fact that research is often carried out with data that is provided in coded form by another data controller has an impact in various places in the chapter. The rights will often have to be exercised via the provider. This is of course different if the research institute has collected the data or human tissue from the participant itself.

6.1 Exercise of rights: when and through which party

This section elaborates in particular on Article 11 GDPR. The fact that it must be possible to *uniquely* identify the participant is not stated literally in Article 11, paragraph 2 of the GDPR, but can be read into it. It is obviously not the intention that someone receives the data from someone else.

The section goes further than strictly necessary in the context of transparency. The website must provide clear information. The last sentence of Article 14 (4) (d) is thus also made applicable to Article 11 situations. In the case of coded data, withdrawal of consent or subsequent objection can always take place via the provider. The section points out that research institutes must provide clear information on this.

6.2 Right of access

This provision elaborates on the possibility of an exemption to Article 15 GDPR. This exemption is legally possible on the basis of Article 89.2 GDPR in conjunction with Article 44 UAVG. In this provision a proportional limitation has been chosen in line with what was stated in the introduction. In general, transparency applies.

6.3 Right to rectification

This provision elaborates on the possibility of an exemption to Article 16 GDPR. This exemption is legally possible on the basis of Article 89.2 GDPR in conjunction with Article 44 UAVG. The same situation applies as mentioned in the previous norm. The restriction on the right to information is in principle permissible in scientific research, but is limited here to when it is necessary for the protection of the participant or not necessary for the integrity of the research data.

6.4 Right to erasure

The restriction on this right in the case of scientific research is included in the GDPR itself (17.3. b, c and d GDPR). The clauses of the first paragraph of Article 17 have been ignored by the Code of Conduct. Thus, the code of conduct promotes the trust of participants but also simplifies the administration for research institutions.

In such a case, data or human tissue must be erased or destroyed, unless one of the exemptions mentioned applies. These exemptions elaborate on the exemptions to the right to erasure in Article 17.3b-d GDPR. The elaboration does not go beyond what is necessary for the integrity of health

research and is sufficiently defined and specific to serve as an adequate explanation/specification of the provision for a Code of Conduct.

However, the Code of Conduct assumes the following: the participant cannot invoke the right to erasure and at the same time continue to participate in the study. Any other conclusion would be absurd. The interpretation of the criteria is therefore to be found in the right to object.

6.5 Right to data portability

There is no separate exemption to this right (Article 20 GDPR) for scientific research under the GDPR itself. The rights described in this section therefore give the participant as many rights as any other data subject. *NB: here we need to look further, 2 things are mixed up: access and portability.* The restriction of those rights that is possible under Article 44 UAVG or inherent in the nature of the GDPR provisions (compare Article 20) has been applied with restraint. The standards stipulate that a restriction is only possible to protect the integrity of the research or the research data, or to protect the participant himself or other participants.

Although the right to a copy and the right to portability are two different rights (15 and 20 GDPR, respectively), the Code of Conduct partly deals with them together. As also stated in the explanatory notes to the norm, the Code of Conduct goes further than the text of Article 20 with regard to portability. The limitation of direct transfer of data to situations where this is 'technically feasible' is mentioned in Recital 68 GDPR.

6.6 Right to object

This section deals with two issues. The data processing must be stopped. This follows from the text of Article 21, paragraph 6. The Code of Conduct does not impose the additional condition that the participant must legitimise this. This would be contrary to the Dutch principle that data processing in scientific research is only possible on the basis of consent or no objection. The fact that this objection can also be made later to the healthcare provider (see chapter 5) is an additional safeguard that the conditions of Article 24 GDPR are met.

Retention is also a form of processing, and therefore the Code of Conduct makes it clear that the data must in principle be deleted if retention serves no other purpose than scientific research. A logical

interpretation of the law does mean that the exemptions to the right to erasure under Article 17.3 GDPR are reflected here, as also explained in connection with the consequences of withdrawing consent (section 4.8). This is elaborated in this provision.

6.7 Dealing with individual findings

The treatment of individual findings in the final chapter has significance both here and for the previous chapters, in particular 2, 3 and 4. Strictly speaking, this is not a data protection right. What is involved, however, is the right to know and not to know information about one's health, a right that is familiar from medical (research) ethics and health law.¹¹⁵ It can therefore be seen as a condition for a proper and transparent processing of data (and human tissue) (Article 5.1a GDPR). The right to be actively informed of such findings is an additional right of the participant compared to the GDPR. When exactly a finding *must* be reported, and when there is a significant risk of findings, is subject to discussion. The Explanatory Memorandum to the WzI recommends that the field should come up with a quality standard on what constitutes a significant risk of individual findings, when this can occur and how this should be dealt with.¹¹⁶ The instructions and advice in the Code of Conduct are derived from the consensus in the field about the responsibility of the investigator for his/her participants.

¹¹⁵ Gezondheidsraad 2014.

¹¹⁶ 2021, 35 844, nr. 3.

7 Publication

Standards for publications concern two aspects: the duty to strive for publication of the results of [scientific research](#), and the principle of publishing results anonymously. These standards give substance to general requirements for scientific research respecting research integrity, and thus also to principles of data protection, such as lawfulness, fairness and transparency.

7.1 Publishing the results of research

Publishing results and making research data accessible are crucial for scientific discussion, ascertaining the truth, and increasing and spreading knowledge and insights. Transparency about results and how they were achieved is therefore an essential feature of *scientific* research and essential for the scientific integrity and scientific and societal value of that research. The publication of research results also justifies recourse to exemptions to the normal data protection regime in scientific research.¹¹⁷ Participants must be able to count on this because of their participation: without the publication of results, participation has little meaning. Researchers thus also give substance to the principle of lawful, proper and transparent data processing under Article 5.1a GDPR.

This Code of Conduct assumes that scientific integrity rules are followed to the fullest extent and does not set any additional rules in this respect. The Code of Conduct for Scientific Integrity sets the standard that research results and data should be made publicly available as much as possible after the research has been completed. Researchers are expected to communicate honestly and to be clear about the limitations of the research and of their own expertise, and to be open and honest about possible conflicts of interest.¹¹⁸ It should be noted that in some forms of research, publication of results cannot be expected, or can only be expected in exceptional cases. Examples of this are research carried out in the context of training or education, and pilot studies.¹¹⁹

7.2 Publishing information about patients or participants

In the context of this Code of Conduct, the protection of personal data and privacy must of course be taken into account when publishing. The rights and interests of the participants involved must also be

¹¹⁷ European Data Protection Supervisor 2020, p. 11-12. See also recital 159 of the GDPR.

¹¹⁸ KNAW e.a., 'Nederlandse gedragscode wetenschappelijke integriteit', <https://easy.dans.knaw.nl>, doi:10.17026/DANS-2CJ-NVWU, 2018 Normen onder 3.4 en 3.6, in het bijzonder norm 45.

¹¹⁹ Note that such research must comply with this Code of Conduct.

weighed against the interest of academic freedom (of expression). The GDPR and the GDPR Implementation Act have separate exemption provisions for this purpose, see Section 85 GDPR in conjunction with Section 43 UAVG. Incidentally, this Code of Conduct assumes a restrictive interpretation of these exemptions: in principle, these provisions are only relevant for scientific publications, not for the confidential sharing of data with other researchers, for example. The exemptions do not alter the fact that data protection principles must be respected and that appropriate safeguards must be put in place for processing for scientific research purposes (ex Article 89.1 GDPR).¹²⁰

In this light, the Code of Conduct states that participants or patients should in principle be anonymous in publications. This principle may only be deviated from if it is necessary from a scientific point of view. Participants or their representatives must in that case give explicit consent for publication.¹²¹ If they have died in the meantime, a careful weighing up of the interests at stake is necessary in the specific case. This approach is in line with the Dutch legal principle of explicit consent for the processing of health data for the purpose of scientific research (Article 24 UAVG) and with the Dutch approach to medical confidentiality after death. The Code of Conduct does not assume vicarious consent by next of kin for the publication of identifying information after death (as is sometimes customary in other countries), because under Dutch law such consent cannot replace the deceased's consent and because it is not always morally desirable to approach next of kin about this either.¹²²

7.3 Disclosure of research data

The principle of anonymity also has an impact on the publication of open data. In addition, the recognisability of healthcare providers in certain studies is a point for attention. The standard is that they are not separately recognisable in the results and data, unless agreed otherwise. From a data protection point of view, this offers an extra safeguard against possible identification of data subjects.

¹²⁰ The letter of the law leaves more room for exceptions for 'academic expression' than this norm provides. The restrictive interpretation chosen here is in line with the view of the EDPS, *preliminary opinion on data protection and scientific research*, January 2020.

¹²¹ Barbour e.a. 2016.

¹²² Ploem, Bak & Linthorst, *Nederlands Tijdschrift Voor Geneeskunde* 2021/165.

8 Management and archiving

This chapter deals with a number of rules for the management and archiving of personal data and human tissue for scientific research. This is how the principle of storage limitation for health research is interpreted, in connection with aspects such as controllership and information for participants which are also dealt with elsewhere in the Code of Conduct. The chapter specifically covers the following standards from the applicable regulations:

- Article 5 par. 1.e GDPR in conjunction with Article 89.1 GDPR in conjunction with Recital 39 GDPR (norm 8.2.1, 8.2.2);
- Code of Conduct for Scientific Integrity, norm 3.3.24 (norm 8.1.1);
- Article 58 Clinical trials - Regulation EU No 536/2014 (norm 8.2.1);
- Public Records Act 1995 (norm 8.2.1); *and*
- Article 7:454 of the Civil Code (norm 8.2.1).

8.1 Securing responsibility for management

Data and human tissue must be carefully managed and archived for a period appropriate to the discipline and methodology.¹²³ The conditions that such management must fulfil are essentially dealt with in other chapters, in particular the chapters on appropriate safeguards (chapter 2) and on controllership (chapter 10). The responsibility for data management should be clearly assigned. Administrators play an important role in realising and respecting the standards in this Code of Conduct. Agreements about this can be laid down in management regulations for collections and/or institutional policies for data and human tissue management. Management regulations are particularly common in the management of human tissue in biobanks. The Control of Human Tissue Act codifies this practice and may set further conditions for it. For research conducted under the responsibility of institutions to which the Public Records Act applies (including universities and UMCs), additional data management conditions apply under the Public Records Act.

¹²³ Code of conduct for scientific integrity, norm 3.3.24.

8.2 Defining retention periods

This section gives an interpretation of the principle of storage restriction and the special status of processing in the context of scientific research (Article 5.1.e GDPR in conjunction with Article 89.1). This is elaborated in the obligation to specify and justify a maximum retention period as a specific guarantee for the protection of the rights of those involved. This retention period must be reviewed periodically (Recital 39 GDPR), unless there is a legal obligation to store or a fixed period has been laid down in the protocol or in the information for participants.

Due to the very different situations of research, the Code of Conduct does not dictate a specific retention period. On this point, no more specification of the GDPR can be offered. As noted, every retention period must be recorded, and it must be possible to justify it. Frameworks and considerations to take into account are:

- Legal retention periods - these take precedence over others:
 - For clinical trials and research with advanced therapeutic medicinal products (ATMPs): 25 and 30 years, respectively, after the end of the trial;¹²⁴
 - For institutions to which the Archives Act applies (e.g. universities and UMCs), from the Archives Act, as laid down in selection lists;¹²⁵
 - For human tissue or data that is also intended or processed for a statutory purpose other than scientific research, any statutory retention period applicable to those other purposes applies. For the medical file, a retention period of 20 years applies, calculated from the time when the last change in the file took place;¹²⁶
- guidelines for retention periods of relevant disciplines, professional groups and supervisors;¹²⁷
- insurance retention periods (e.g. for research that is subject to the WMO);

¹²⁴ Article 58 Clinical trials - Regulation EU No 536/2014.

¹²⁵ Archives Act 1995.

¹²⁶ Article 7:454 of the Civil Code.

¹²⁷ The CCMO has stated the following for research that is subject to the WMO obligation: <https://www.ccmo.nl/onderzoekers/standaardonderzoeksdossier/e-informatie-proefpersonen/e1-e2-informatiebrief-en-toestemmingsformulier-proefpersonen/e1-e2c-vragen-en-antwoorden-over-de-gegevenssectie-van-het-model-proefpersoneninformatie-voor-proefpersonen-van-16-jaar-en-ouder-volwassenen> [15-6-2021]: 'No retention period has been laid down in legislation and regulations for other WMO studies (no drug studies). The CCMO considers a retention period of at least 15 years acceptable, provided it is substantiated in the protocol. If, in the case of specific studies, a shorter retention period than that referred to above is sufficient, the CCMO considers it appropriate to apply a shorter period. In principle, the retention periods for data at the research site and at the sponsor are the same. If these are different, the model PIF offers the option of stating the storage period at the research site and at the sponsor separately. The protocol should contain a further specification of the data to be retained at the research site and at the sponsor during the retention period. Such details do not need to be included in the PIF.'

- Institutional policy on data and human tissue management;
- possible replication and validation of research, among other things because of retention periods that may be required by scientific publications: ten years after publication is a prevailing norm;¹²⁸
and
- use and re-use for future scientific research.

This Code of Conduct specifically deals with the handling of anonymous data, personal data and human tissue. For the sake of completeness, it should be noted that personal data and human tissue are not the only things to be archived for fair and responsible research. Other aspects of the study such as the protocol, syntaxes and the like should also be carefully archived. See also the guideline for *responsible epidemiological research practice*.¹²⁹

8.3 Appropriate safeguards for archiving

This norm points out to researchers the importance of taking appropriate precautions as soon as data and human tissue are archived. Please refer to chapter 2 for the justification.

8.4 Responsibilities for institutions

The first norm, which obliges institutions to ensure a research infrastructure in which proper management of data and human tissue is the rule and is facilitated, is a duty of care from the Code of Conduct for Scientific Integrity.¹³⁰ This norm extends to and includes the perspective of data protection which is central to this Code of Conduct. Secondly, this section obliges institutions to secure responsibilities within the organisation for the implementation of and compliance with standards formulated in this Code of Conduct.

Obligations and responsibilities arising in respect of data and human tissue management, such as the Public Records Act and Wz (in the future), are not elaborated on in this section.

¹²⁸ Many (medical) scientific journals require a *data availability statement* for publications. Journals can also require a minimum retention period as part of this. A retention period of at least ten years for the source data underlying the results is usual. See 'ICMJE | Recommendations for the Conduct, Reporting, Editing and Publication of Scholarly Work in Medical Journals', www.icmje.org.

¹²⁹ Swaen e.a., *Journal of Clinical Epidemiology* 2018/100.

¹³⁰ KNAW e.a., 'Nederlandse gedragscode wetenschappelijke integriteit', <https://easy.dans.knaw.nl>, doi:10.17026/DANS-2CJ-NVWU, 2018. Par. 4.4, no. 11.

9 Use and re-use of research data and human tissue for new research

This chapter addresses the use and re-use of research data and human tissue for new research. In particular, the chapter covers the following standards from the applicable regulations:

- Code of Conduct for Scientific Integrity, 3.3.25 (norm 9.1.1);
- Article 5.1e GDPR in conjunction with Article 89.1 GDPR (norm 9.1.1);
- Article 13 par. 2.a GDPR in conjunction with Recitals 39, 78 and 156 GDPR (norm 9.2.2).

The use and re-use of data and human tissue for new scientific research is a standard part of scientific research. Moreover, facilitating the re-use of research data is encouraged under the banner of Open Science and FAIR data management, and institutionalised among other things through requirements imposed by research funding bodies. Responsible re-use is also a way to optimally exploit the scientific and societal value of research data and possibly reduce the burden on participants. Scientific integrity rules prescribe that re-use should be facilitated where appropriate and that research data should be made available 'as open as possible, as closed as necessary'.¹³¹ Researchers are expected to contribute to making data discoverable, accessible, interoperable and reusable where appropriate, in accordance with FAIR principles.¹³²

Of course, the conditions of the GDPR must still be met. The standards formulated in previous chapters also apply to these actions with data and human tissue. What this means exactly in the context of re-use or supply is explained in this chapter.

9.1 Anticipating use and re-use for future research

It is important to anticipate possible (re)use in the design of research and the collection of data and human tissue from participants. The standards specify the central points of attention. The legal foundations are given in the sections to which the standards refer.

¹³¹ Elaboration of Code of Conduct for Scientific Integrity, norm 3.2.11.

¹³² Code of conduct for scientific integrity, norm 3.3.25.

9.2 Complying with data protection rules when used and re-used in new research

For the conduct of new research involving the (re-)use of data and human tissue, the rules of this code of conduct apply accordingly. It is therefore important to check whether the rules in other chapters (in particular, the conditions of chapter 4 or 5) have been complied with for this re-use. This will be easier if possible (re)use is anticipated earlier. In such a case, it will be easier to build on previously requested consent from participants and, if necessary, it will be easier to inform participants about the new research. The legal foundations are given in the sections to which the standards refer.

Article 5.1.b GDPR provides an exemption to the principle of purpose limitation. However, this exemption is only meaningful if the previous purpose of the data processing is something other than scientific research. Re-use, use or issue for new health research cannot therefore be legitimised by invoking this.

Incidentally, validation and replication research (including meta-analyses, *systematic reviews* and the like) do not in principle count as "new research". Such research can be considered compatible with the original research purposes provided the conduct of this research meets the conditions of Article 89.1 GDPR.¹³³ If new data controllers are involved in this research, the participants will have to be adequately informed. See also chapters 3 and 4 .

¹³³ Article 5.1b GDPR.

10 Controllershship

This chapter covers Articles 4.7, 4.8, 26 and 28 GDPR. The EDPB guidelines on processor and controller have also been taken into account.¹³⁴

As the chapter repeatedly points out, these are merely guidelines. More specification cannot be given in the chapter. Researchers are advised always to consult the specialists of their organisation for the design of cooperation agreements.

10.1 Main rule: when controller

Here, a translation of the GDPR terms for standard research situations has been provided that is as comprehensible as possible. The explanation makes it clear that a person can also be a data controller if they do not receive any personal data themselves. The example is taken from the EDPB Guidelines.¹³⁵

Norm 10.1.2 deals with the doctor who is attached to a healthcare provider via a so-called *Medisch Specialistisch Bedrijf*. This 'independent specialist' is not 'attached to' a research institute. As a rule, there will be a dependency on the support of the healthcare provider, making the latter jointly responsible. After all, the healthcare provider is already responsible for the data processing in the primary process of the doctor in question (patient care). It would not be in keeping with the responsibility of the healthcare provider to then be considered the processor of the doctor for the part of the scientific research that is initiated by the doctor or in which he is involved. In general, the code of conduct is reluctant to designate an organisation as a processor in the case of health research, see below.

10.2 Joint controllers

If researchers from several research institutes collaborate on the protocol, then the purpose and means of processing are jointly determined, and the person responsible for processing is also jointly responsible.

¹³⁴ European Data Protection Board 2021.

¹³⁵ European Data Protection Board 2021, p. 16.; HvJ EU 10 juli 2018, ECLI:EU:C:2018:551 (*Jehovan todistajat*, C-25/17), p. 18.

However, there may also be other circumstances under which one can become a joint controller. This is definitely the case under the circumstance mentioned in the norm. After all, it does not say explicitly 'Only if researchers of ...'.

The explanatory memorandum refers to those other circumstances. This is very casuistic and cannot be dealt with in the Code of Conduct. It follows from norm 5.7 that cooperation in health research must always be laid down contractually and that the researcher must call in specialist help for this. The latter will then also have to assess whether a joint controllership arises for part of the processing as a result of the collaboration.

The norm has been formulated in such a way that it is clear that joint controllership does not mean that one becomes the other party's sole processor. Joint controllership only applies to the part where the parties have become dependent on each other for the purpose and means. In norm 5.7 it is recommended that, for example, an appendix to the agreement should describe for which purposes they are jointly responsible for processing and for which purposes they are not.

Incidentally, in large research consortia there is still a great deal of confusion about joint controllership. Various partners from different disciplines have worked on the proposal together and received subsidies to carry out or contribute to their own 'work package'. They depend on each other for implementation. Data processing is carried out by only a few partners, and the specific research protocols are determined during the course of the project. It would be going too far to make all partners, such as those in an ethical or legal role advising or supporting certain software developments, jointly responsible for processing. The EDPB guidelines, which also address the division of controllership between only a few involved parties as a result of case law, do not provide any clarity on this. The elaboration of a webinar on this subject aims to provide more clarity in the course of 2021.¹³⁶

Norm 10.2.2 describes the role of the provider in terms of whether or not it is jointly responsible for processing data for the purposes of the research. As also follows from the EDPB guidelines, this is not automatically the case,¹³⁷ but only if the conditions for joint controllership are met. The addition of 'inseparable from it' is derived from the criterion introduced in case law, which offers a refinement of determining the purpose and means together.

¹³⁶ <https://www.lygature.org/webinar-joint-controllers-large-research-consortia>

¹³⁷ The Rathenau seems to have a different opinion on joint controllers. There the provider is by definition also joint controller of the research. This point of view is not backed up by the GDPR and the Opinion of the EDPB and is not used here, see: Rathenau Instituut 2020, p. 9. 92/3

As in the case of joint controllers in large research consortia, it is difficult to determine here exactly where the boundary lies between provider (controller 1) - recipient (new controller 2) and joint controllers. The Dutch view is that the research institute to which the PI is linked in a clinical trial is always jointly responsible for the data processing of the sponsor of the trial, or at least, so it must be assumed, for the data that are collected by this PI in the context of the trial and submitted to the sponsor in pseudonymised form. In Belgium, on the other hand, the starting point is the provider (data controller 1 = the PI or the research institute) - recipient (new data controller 2 = the sponsor) construction. There is something to be said for both views. The Belgian approach seems to be more in line with the guidelines of the EDPB.¹³⁸ To be a joint data controller, one must have worked jointly on the protocol, the main norm of this chapter. It also makes the situation a lot clearer for the sponsor. There is then no web of joint controllers, each for their own data, while the analysis of the data must take place on the whole data set. The added value for the participants also seems to be absent. The rights of the participant can also be passed on to the latter in the provider-receiver construction (see Article 19 GDPR).

On the other hand, the principle of 'inseparability' from case law is not applicable. Without the PI, the sponsor does not receive the data. But there are several PIs, and others could be contracted as well. The fact that one makes a significant contribution does not mean it is so essential that it has a manifest impact on the determination of the purposes and means of the data processing.¹³⁹

The Code of Conduct does not make a choice in this discussion.

The strongly casuistic perspective, except for the obvious joint drafting of a research protocol, of the criterion 'inextricably linked' in the chain of the research data has been intended to be expressed in the norm and explanation in more or less understandable terms for researchers. However, this remains a tailor-made approach for which the lawyers of the research institute, taking into account the EDPB guidelines, among others, must provide an appropriate solution.

Norm 10.2.3 is in line with the recommendation of the EDPB. The content of that agreement is not elaborated on, as that is also too case-specific and falls outside the scope of this Code of Conduct.

The explanatory notes to 10.2.3 are in line with the previous Code of Conduct provisions on transparency and provide a practicable interpretation of the EDPB guidelines on this issue.¹⁴⁰

¹³⁸ European Data Protection Board 2021, p. 21-22.

¹³⁹ European Data Protection Board 2021, p. 18.

¹⁴⁰ European Data Protection Board 2021/177–183.

10.3 Processors

This section makes the position of a processor clear to researchers. Norm 10.5.1 shows the connection with Article 28.3 GDPR. The processor agreement is not further specified. This is not relevant for researchers and should be left to their lawyers. There are no specifics here for health research, and the processor agreement therefore falls outside the scope of this Code of Conduct.

The section makes it clear in the various standards, perhaps superfluously, that it is not possible to escape the need for having one's own legal basis for processing when determining ends and means by acting as a processor and using someone else's basis.

Apart from the issue of the basis, scientific research requires a form of autonomy in order to comply with the Code of Conduct for Scientific Integrity, which is incompatible with acting solely on instructions. Therefore, health research according to this Code of Conduct cannot be carried out by a processor. This does not mean that a processor cannot use scientific methods, but that is not health research as a special form of scientific research. That is expressed in norm 10.3.1.

10.4 Securing distinction between different roles within one organisation

This section covers how a situation that occurs frequently in research can be carried out within the boundaries of the strict controller-processor division. A research institution will usually have multiple processors. It is considered acceptable that in a particular study, the research institution first acts as a processor for one or more external providers and makes the already processed data available to researchers within the same research institution on behalf of the provider. The Explanatory Memorandum sets out the limits, namely only when there are "Chinese walls" between the two processing operations, using a metaphor borrowed from the financial compliance literature.¹⁴¹ This prevents a situation that the AP ruled on in the *Snappet* case.¹⁴²

For the researchers, the Code of Conduct in this section makes it clear that in the case of secondary use within one organisation, access to the research data must be as limited as possible (see also chapters 3 and 5) but that there need not be a 'Chinese wall'. This is not possible either.

¹⁴¹ Alferink, *Onderneming en Financiering* 2004/13.

¹⁴² Authority for the Protection of Personal Data, 14 July 2014, research *Snappet*, para. 5.1.

10.5 Defining roles in agreements

This section is self-explanatory and does not require any explanation in the legal justification.

11 Assurance, monitoring and implementation

11.1 Security

This section deals with additional mechanisms that contribute to the effective implementation of the Code of Conduct. This is not a direct specification of specific GDPR or Dutch regulations. That has already been done.

11.2 Monitoring compliance with the Code of Conduct

Health research does not take place in some kind of free space. Various forms of assessment of the ethical and legal aspects of the research are already taking place. The health research carried out by those following the Code of Conduct is usually subsidised. Both methodological and ethical aspects will be addressed when the grant is awarded. This is one of the reasons why ZonMw made an important financial contribution to the Code of Conduct. The code of conduct offers an unambiguous instrument for assessing health research in the application and grant settlement phases. This naturally affects how applications are drawn up and how research is carried out. At the end of the research, the conditions are set for publication of the results. Then one has to justify that the research was carried out in accordance with the applicable standards for the protection of participants. In between, there is a wide range of legal experts and review and assessment committees, some of which are also guaranteed by law, such as the MECs under the WMO and the WZL in the future, which assess the research and request guarantees for the conduct of the research, also in the cooperation agreement or DTAs and similar instruments in the case of multicentre research. In addition, there is the role of the DPO which every research institution should have at its disposal.

12 References

Van Agt, *Medisch Contact* 21 oktober 2020

F. van Agt, 'Stop de wildgroei aan lokale METC's', *Medisch Contact* 21 oktober 2020, www.medischcontact.nl.

Alferink, *Onderneming en Financiering* 2004/13

T.G.A. Alferink, 'Chinese Walls: de stand van zaken', *Onderneming en Financiering* 2004/13, 63, p. 4.

Article 29 Data Protection Working Party 2014

Article 29 Data Protection Working Party, *Opinion 05/2014 on Anonymisation Techniques*, Art. 29 WP 2014.

Barbour e.a. 2016

V. Barbour e.a., *Journals' Best Practices for Ensuring Consent for Publishing Medical Case Reports*, Committee on Publication Ethics 2016, <https://publicationethics.org>, doi:10.24318/cope.2019.1.6.

Bauman, Mellins & Klitzman, *The Journal of Law, Medicine & Ethics: A Journal of the American Society of Law, Medicine & Ethics* 2020/48

L.J. Bauman, C.A. Mellins & R. Klitzman, 'Whether to Waive Parental Permission in HIV Prevention Research Among Adolescents: Ethical and Legal Considerations', *The Journal of Law, Medicine & Ethics: A Journal of the American Society of Law, Medicine & Ethics* 2020/48, 1, p. 188–201, doi:10.1177/1073110520917010.

Boeckhout e.a. 2020

M. Boeckhout e.a., Ethische toetsing niet-WMO-plichtig onderzoek: tijd en ruimte voor verbetering, *MLCF* 2020, <https://mlcf.eu>.

Bouter, Dongen & Zielhuis 2005

L.M. Bouter, M.C.J.M. van Dongen & G.A. Zielhuis, *Epidemiologisch onderzoek: opzet en interpretatie*, Bohn Stafleu Van Loghum 2005, <https://research.vu.nl>.

Coebergh e.a., *European Journal of Cancer* 2015/51

J.W. Coebergh e.a., 'EUROCOURSE recipe for cancer surveillance by visible population-based cancer RegisTrees® in Europe: From roots to fruits', *European Journal of Cancer* 2015/51, 9, p. 1050–1063, doi:10.1016/j.ejca.2015.02.017.

Commissie Regelgeving Onderzoek 2018

Commissie Regelgeving Onderzoek, *COREON Statement Wetenschappelijk onderzoek*, 2018.

European Commission 2020

European Commission, Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation, Brussel: European Commission 2020, <https://eur-lex.europa.eu>.

European Data Protection Board 2020

European Data Protection Board, *Guidelines 05/2020 on consent under Regulation 2016/679* | European Data Protection Board, Brussel: EDPB 2020, <https://edpb.europa.eu>.

European Data Protection Board 2021

European Data Protection Board, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, Brussel: EDPB 2021, <https://edpb.europa.eu>.

European Data Protection Board (EDPB) 2021

European Data Protection Board (EDPB), EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research, 2021, <https://edpb.europa.eu>.

European Data Protection Supervisor 2020

European Data Protection Supervisor, *A Preliminary Opinion on data protection and scientific research*, Brussel: EDPS 2020, <https://edps.europa.eu>.

Flores e.a., *Nursing outlook* 2018/66

D. Flores e.a., 'Obtaining Waivers of Parental Consent: A Strategy Endorsed by Gay, Bisexual, and Queer Adolescent Males for Health Prevention Research', *Nursing outlook* 2018/66, 2, p. 138–148, doi:10.1016/j.outlook.2017.09.001.

Gezondheidsraad 2014

Gezondheidsraad, *Nevenbevindingen bij diagnostiek in de patiëntenzorg* (advies), Ministerie van Volksgezondheid, Welzijn en Sport 2014, www.gezondheidsraad.nl.

Groos & Veen, *European Data Protection Law Review* 2020/6

D. Groos & E.-B. van Veen, 'Anonymised Data and the Rule of Law', *European Data Protection Law Review* 2020/6, 4, p. 498–508, doi:10.21552/edpl/2020/4/6.

Guidelines on Transparency under Regulation 2016/679 (wp260rev.01)

Guidelines on Transparency under Regulation 2016/679 (wp260rev.01), , <https://ec.europa.eu>.

Hallinan, *Life Sciences, Society and Policy* 2020/16

D. Hallinan, 'Broad consent under the GDPR: an optimistic perspective on a bright future', *Life Sciences, Society and Policy* 2020/16, 1, p. 1, doi:10.1186/s40504-019-0096-3.

'Handreiking Hergebruik van zorggegevens voor wetenschappelijk onderzoek 14-10-2020'
'Handreiking Hergebruik van zorggegevens voor wetenschappelijk onderzoek 14-10-2020', , p. 8.

Hoepman, J.-H. 2018

Hoepman, J.-H., *Privacyontwerpstrategieën (Het Blauwe Boekje)*, Nijmegen : Radboud Universiteit 2018, <http://hdl.handle.net>.

Konijnenburg, Teeuw & Ploem, *European Journal of Pediatrics* 2015/174

E.M.M.H. van Konijnenburg, A.H. Teeuw & M.C. Ploem, 'Data research on child abuse and neglect without informed consent? Balancing interests under Dutch law', *European Journal of Pediatrics* 2015/174, 12, p. 1573, doi:10.1007/s00431-015-2649-7.

Liu e.a., *Journal of Adolescent Health* 2017/61

C. Liu e.a., 'The Effects of Requiring Parental Consent for Research on Adolescents' Risk Behaviors: A Meta-analysis', *Journal of Adolescent Health* 2017/61, 1, p. 45–52, doi:10.1016/j.jadohealth.2017.01.015.

Ministerie van Volksgezondheid 2005

W. en S. Ministerie van Volksgezondheid, *CCMO-notitie Definitie medisch-wetenschappelijk onderzoek* (publicatie), Centrale Commissie Mensgebonden Onderzoek 2005, www.ccmo.nl.

Ministerie van Volksgezondheid 2020

W. en S. Ministerie van Volksgezondheid, *CCMO-notitie Stappenplannen inzake uitgestelde toestemming ('deferred consent') bij onderzoek in noodsituaties - Publicatie - Centrale Commissie Mensgebonden Onderzoek* (publicatie), Den Haag: CCMO 2020, www.ccmo.nl.

Ploem, Bak & Linthorst, *Nederlands Tijdschrift Voor Geneeskunde* 2021/165

C.M.C. Ploem, M.A.R. Bak & G.E. Linthorst, 'Casuïstiek van overleden patiënten', *Nederlands Tijdschrift Voor Geneeskunde* 2021/165, p. D5685.

Ploem, Rigter & Gevers, *Tijdschrift voor Gezondheidsrecht* 2020/44

M.C. Ploem, T. Rigter & J.K.M. Gevers, 'Medisch data-onderzoek in het AVG-tijdperk: een zoektocht naar de juiste regels', *Tijdschrift voor Gezondheidsrecht* 2020/44, 2, p. 162–181, doi:10.5553/TvGR/016508742020044002004.

Rathenau Instituut 2020

Rathenau Instituut, *Verbeterpunten voor datasolidariteit met gezondheidsgegevens*, Den Haag 2020, p. 9, www.rathenau.nl.

Swaen e.a., *Journal of Clinical Epidemiology* 2018/100

G.M.H. Swaen e.a., 'Responsible Epidemiologic Research Practice: a guideline developed by a working group of the Netherlands Epidemiological Society', *Journal of Clinical Epidemiology* 2018/100, p. 111–119, doi:10.1016/j.jclinepi.2018.02.010.

Teague e.a., *BMC Medical Research Methodology* 2018/18

S. Teague e.a., 'Retention strategies in longitudinal cohort studies: a systematic review and meta-analysis', *BMC Medical Research Methodology* 2018/18, 1, p. 151, doi:10.1186/s12874-018-0586-7.

Timmers e.a., *Medical Law Review* 2019/27

M. Timmers e.a., 'Will the Eu Data Protection Regulation 2016/679 Inhibit Critical Care Research?', *Medical Law Review* 2019/27, 1, p. 59–78, doi:10.1093/medlaw/fwy023.

HvJ EU 19 oktober 2016, ECLI:EU:C:2016:779 (*Breyer, C-582/14*).

HvJ EU 10 juli 2018, ECLI:EU:C:2018:551 (*Jehovan todistajat, C-25/17*).

'Nederlandse gedragscode wetenschappelijke integriteit'

KNAW e.a., 'Nederlandse gedragscode wetenschappelijke integriteit', <https://easy.dans.knaw.nl>, doi:10.17026/DANS-2CJ-NVWU, 2018.

Appendix A: Overview of relevant legal articles per section

This table shows which relevant provisions are elaborated into standards in part 1 of the Code of Conduct.

Where in particular	GDPR (EU General Data Protection Regulation) / UAVG (Dutch GDPR Implementing act) / WGBO (Dutch Act on Medical Treatment Contracts)
Definitions	GDPR 4.1, GDPR 4.5, GDPR 4.7, GDPR 4.8
Section 1.1	GDPR 5.1, GDPR 24, GDPR 25, GDPR 89.1
Section 1.3	GDPR 30, GDPR 35
Section 2.1	GDPR 5.1.c
Section 2.2	GDPR 25,89.1
Section 2.4	GDPR 24, GDPR 25, GDPR 89.1
Section 2.5	GDPR 24, GDPR 25, GDPR 89.1
Section 3.1	GDPR 13, GDPR 14
Section 3.2	GDPR 11, GDPR 14b
Section 3.3	GDPR 13.1 . c, GDPR 13.1 . d, GDPR 13.1.e
Section 4.1	GDPR 5.1.b, GDPR 6.1.e, GDPR 6.1.f
Section 4.2	GDPR 4.11, 6.1a, GDPR 7, GDPR 9.2a
Section 4.3	GDPR 4.11, 13
Section 4.4	GDPR 4.11
Section 4.6	GDPR 4.11,7.4
Section 4.7	GDPR 4.11, GDPR 7.1

Section4 .8	GDPR 4.11, GDPR 7. 3
Section 5.1	GDPR 5.1.b, WGBO 7:457
Section 5.2	GDPR 9.2.a
Section 5.3	GDPR 12,13,19 , WGBO 7:457
Section 5.4	UAVG 24, UAVG28 , WGBO 7:458
Section 5.5	UAVG 24, UAVG28 , WGBO 7:458
Section 5.6	GDPR 13, WGBO 7:457, WGBO 7:458
Section 5.7	UAVG 24, UAVG 28, WGBO 7:457, WGBO 7:458
Section 6.1	GDPR 11, GDPR 14
Section 6.2	GDPR 15, GDPR 89.2, UAVG 44
Section 6.3	AVG16, UAVG 89.2,44
Section 6.4	GDPR 17.3. b, GDPR 17.3.c, GDPR 17.3.d
Section 6.5	GDPR 15,20
Section 6.6	GDPR 21.6,24, GDPR 17.3
Section 7.1	GDPR 5.1.a
Section 7.2	GDPR 89.1
Section 8.2	GDPR 5.1.e, GDPR 89.1
Section 9.1	GDPR 5.1.e, GDPR 89.1
Section 9.2	GDPR 89.1
Chapter 10	GDPR 4.7, GDPR 4.8, GDPR 26, GDPR 28

Appendix B: Establishment of the Code of Conduct

COREON took the initiative to revise the 2004 Health Research Code of Practice. The update started in November 2019 and was co-sponsored by ZonMw (project number 34009101), NFU, the programme Care Evaluation and Appropriate Use (ZE&GG), the Interfaculty Consultation on General Practice (IOH) and BBMRI-NL.

For the update, COREON entrusted the implementation and daily management of the project to the MLC Foundation (Mr Evert-Ben van Veen and Dr Martin Boeckhout). In addition, COREON formed a core group of lawyers, ethicists, a data protection officer and researchers from various organisations in the health research field, accompanied by an independent technical chairman. The core group consisted of the following members:

- Paul Dalhuisen - Lawyer at Medisch Spectrum Twente
- Dr Michel Paardekooper - Data Protection Officer at Amsterdam UMC
- Corrette Ploem - Special Appointed Professor of Law, Health Care Technology and Medicine because of the Royal Dutch Medical Association at the Faculty of Law, and Associate Professor of Health Law at Amsterdam UMC, University of Amsterdam
- Prof. Sabine Siesling - Professor of Outcomes Research and Personalized Cancer Care at the University of Twente and senior researcher at IKNL
- Dr. Ghislaine van Thiel - Associate Professor of Medical Ethics at UMC Utrecht
- Roy Tomeij - independent chairman

Jasper Bovenberg and Marie-José Bonthuis were also involved in earlier stages of the Core Group.

The Core Group met 19 times. At each meeting the Core Group commented on documents proposed by the MLC Foundation and the reflections on the input from the Sounding Board and other organisations following the public consultation (see below). The Core Group agreed on, and supports, the content of the standards in Part 1 of the Code of Conduct. Part 2 of the Code of Conduct was marginally assessed by the Core Group. Specific input was given by Paul Dalhuisen and Michel Paardekooper.

In addition, a sounding board group was set up with broad representation from involved organisations and data subjects. The following organisations participated:

- Central Committee on Research Involving Human Subjects (CCMO)
- Committee on Regulation of Health Research (COREON)
- Dutch Clinical Research Foundation (DCRF)
- Federation of Medical Specialists (FMS)
- Health-RI
- Interfaculty Consultation on Family Medicine (IOH-R)
- Royal Netherlands Academy of Arts and Sciences (KNAW)
- Ministry of Education, Culture and Science (OCW)
- Ministry of Health, Welfare and Sport (VWS)
- National Ethics Council for Social and Behavioural Sciences (Nethics)
- Netherlands Federation of University Medical Centres (NFU)
- Netherlands Association of Hospitals (NVZ)
- Dutch Association of Medical Ethics Review Committees (NVMETC)
- Dutch Nationwide Pathology Databank (PALGA)
- Healthcare Evaluation and Appropriate Use Programme (ZE&GG)
- National Institute for Public Health and the Environment (RIVM)
- Cooperating Top Clinical Training Hospitals (STZ)
- Universities of The Netherlands (UNL)
- Netherlands Organisation for Health Research and Development (ZonMw)

There were three meetings of the sounding board group. The emphasis was on testing the readability and usability of the draft Code of Conduct, but the main points of the standards were also discussed in terms of content. These meetings were followed by meetings of the COREON members. In June 2021 a readability session took place. This allowed researchers from the COREON network to test the draft for readability for the intended target group.

In July 2021, the draft Code of Conduct was released for public consultation. Organisations and individuals were given the opportunity to give their general reaction to it. In August 2021, the opportunity to comment on the legal justification followed. In total, 14 organisations and individuals responded. One more reaction was received.

On 3 January 2022 this version of the Code of Conduct was presented by MLCF to COREON as initiator.