



## CODE OF CONDUCT for HEALTH RESEARCH

### Chapter 1; Definition of terms

In Article 1 the terms used in the Code of Conduct are defined. The definitions are technical. They are in part the concepts used in the WBP (Act on the Protection of Personal Data) and the WGBO (Act on the Medical Treatment Contract) but they are more specific. This is due to the range of application and the structure of this Code of Conduct. Thus the range of application is broader than that of the WBP and the WGBO. This Code of Conduct also applies for anonymous data, whereas the WBP and the WGBO are only applicable to personal data.

#### *Section a*

In section a, the range of application of the Code of Conduct is described. This is in first instance very broad. However, this Code is an elaboration of that which was laid down in the WGBO about the use of patient data for scientific research. For these data the strict standards of professional confidentiality apply. For health research other sources are also used. For example the Municipal Population Registry (GBA), general surveys, and so on. In these cases the strict standards of professional confidentiality do not apply directly. The general standards of the WBP are considered sufficient. Furthermore, for the so-called “special personal data”, a specific standard applies that closely resembles that of professional confidentiality but nevertheless is not exactly the same. Data on race, health and heredity are considered to be special personal data. At all times however the WBP assumes that this standard will be subordinate to the stricter regulations of professional confidentiality.

If this Code should apply for all data that can be used in health-scientific research, the Code would have to use two systems of standards to keep it from being too restrictive: one for the data which are subject to professional

confidentiality and one for data which are not subject to professional confidentiality. This would yield an exceedingly complicated set of regulations. For this reason the Code is restricted to the first type of data. For this purpose professional confidentiality as it is defined in the Law BIG (Individual health professionals Act) is used as the basis in order to ensure that data that are not directly covered by WGBO, but still are subject to professional confidentiality, will also fall under this Code. As a result, this Code covers all data which fall under professional confidentiality in individual health care. For research with other types of data, which are not subject to professional confidentiality, a different Code will be applied. This was drawn up under the auspices of NOW/KNAW and presented to VSNU in April 2003. It can serve as the basis for all scientific research with (personal) data whenever the data are not covered by professional confidentiality. The KNAW/NOW/VSNU Code uses the same concepts as the FMWV Code of Conduct described here.

However this Code would still be too broad without supplementary restrictions. Health research can also be understood to mean an investigation that is already subject to a special law: the Medical Research involving Human Subjects Act (WMO). The range of application of WMO, which section A refers to, is as follows: "medical research in which persons are subjected to treatment or are required to behave in a certain manner". For this type of investigation the patient or test person undergoes certain procedures in order to obtain specific data. For health research that falls under the Code of Conduct, this is not the case. The data are already available, for example as a result of a treatment regimen which the patient has already undergone or previous health-scientific research as described in the WMO.

It is still however scientific research.

This research must be differentiated from quality control, although scientific methods are also used for the latter. In the case of quality control by care

providers, the procedures executed are evaluated by means of (patient) data obtained from the procedures. Quality control is a continuous process carried out by care providers in order to improve patient care. Patients may assume that such evaluations for quality control take place.

The aim of scientific research is the publication of generally applicable information. Sometimes it will be such that it is immediately applicable, also by others, in order to improve the quality of care, but often the path to application in clinical practice will be much longer, whereby the findings of others will also play a role.

#### *Sections b-c*

The concepts in sections b and c do not exist in the WBP. One can differentiate between health research (in general) and “the investigation” (a specific research project). The Code of Conduct is about the obligations of the researchers involved in a specific investigation, but also their obligations with respect to research in general. (For this aspect, see Chapter 2)

#### *Sections d-i*

Sections d-i define the actors who are involved in the investigation.

In section d, the basic assumption is that the researcher does not have a relationship with the patient. Of course a care provider (see e) can carry out research himself with the help of the data which he supervises.

According to the WGBO the care provider (e) can be a person, such as a doctor or a psychotherapist, but also the institution where the medical treatments or so-called related (nursing) activities take place. This Code is meant indirectly for the care provider as institution (for instance, Article 2.7) and directly for the individual care provider in Article 2.11. If the care provider carries out research with data on his own patients, Article 2.11 is applicable, unless the processing of the data

occurs within the framework of evaluation of the quality of the care, which can be considered the task of a good care provider.

The most important reason why care providers are included in this Code is the fact that the decision of the patient to allow his data to be used for scientific research (the so-called Right to Consent) must be registered by his care provider (individual or institution). For this reason the care provider is referred to in a number of places.

The concept *controller* (f) comes from the WBP. The researcher often works within a larger organization. The controller in the sense of the WBP is therefore not always the researcher but can also be the hierarchical head of the discipline, department or the research institute where the researcher works. Of course this person (professor) can himself also be a researcher in the sense of the Code. The controller has the obligation to make sure that data are processed in a legitimate manner. For research data, this is the case when the researchers within the organization work according to this Code of Conduct. The head, the controller, must create the framework for this and he must see to it that compliance occurs. See also Article 2.1.

The WBP follows the dynamics of data streams. This means among others that if two organizations cooperate with each other, there can also be two controllers who are responsible for the mutual processing of data that results from this cooperation. This will be the case especially if the cooperation takes place on the basis of equality. If however the two organizations form a client-supplier relationship, then one could make a distinction. Then each organization is responsible for the data which is processed – in accordance with the agreed relationship – within one's own organization and is supplied to the other.

The term *processor* (g) is also taken from the WBP. A processor can be a person or an organization. The determining factor is the fact that the processor himself does not have authority over the processing but is subject to the instructions of the controller and processes data only for the aims of the controller. Thus

organizations can act as links between the care provider and the researcher and can carry out procedures with data within that framework. An example of such an organization is the Registration Network of Family Practitioners in Limburg. This organization manages an automated case registry which serves as random sample framework for scientific research and education in health care.<sup>1</sup>

The definition of *the data subject* (h) is obvious.

The concept *supplier* does not have an equivalent in the WBP. A supplier can be a care provider or someone else who has a relevant database containing data that the researcher would like to use, e.g. the CBS or the CBG. One research investigation can of course make use of various suppliers.

### *Sections j-q*

In section j-q the various categories of data are defined. This is probably the most complex part of the Code of Conduct. The distinctions discussed here are relevant for various parts of the Code. It is therefore important to describe them in more detail. For a good understanding the following must first be considered. The basic principle of this Code of Conduct, in accordance with that of the WBP, is that the form of the research investigation must always be such that there is the least possible interference in the personal life of the data subject. Preferably anonymous data must be used and only when that is not possible, may one use data that are more precarious from the standpoint of privacy. This demands a precise definition of the various categories.

### *Personal data versus anonymous data*

As mentioned previously, the WBP and the WGBO cover only personal data whereas the Code also concerns anonymous data. This is the first distinction that

---

<sup>1</sup> Another example is the Comprehensive Cancer Centre on the regional level and the Dutch Association of Comprehensive Cancer Centres on the national level.

must be explained. Within the two categories there are also subcategories. They will be described later.

Anonymous data and personal data are opposite concepts in the WBP.

Anonymous data are not personal data. The WBP defines personal data as data on an identified or identifiable person. Identified is clear. That means that there are directly identifying characteristics tied to the data. Identifiable means that the data are indirectly identifying. Indirectly identifying data do not lead directly to the identity of the data subject but they do contain sufficient identifying factors that the identity of the data subject can be determined without spending disproportionate amounts of time and effort. For a researcher these data will presumably be just as anonymous as “real” anonymous data. According to the WBP however “disproportionate amounts of time and effort” will rarely be the case. That is why these data, due to the possibility of identification - no matter how abstract, must be considered as personal data.

For the degree of being identifiable, a distinction can be made between:

- The nature of the data

and

- The context within which they are used, the means available to the researcher.

As far as the nature of the data is concerned: there is no general formula. As a datum acquires more specific characteristics, it comes closer – either in combination with other data or not – to becoming an identifying datum. *The profession “Minister President” is without a doubt identifying. The occupation “violin maker” becomes identifying when combined with the first two numbers of the postal code.*

With respect to the context within which the data are used: In WBP terms this means the possibilities of the controller, as previously described. Article 2.1 paragraph b ensures that 'dams', as it were, have been thrown up between the various databases found within the research organization. Researchers must consider the research databases as separate entities.

One database for one specific investigation may only be used for another research project if this occurs in accordance with the conditions of this Code of Conduct. This prevents the problem that all data within an organization must be considered as one entity, so that within such an organization there is no longer anonymous data. Only the possibilities of this researcher with this data are important. Technical and organizational measures must make sure that this happens. In the explanation of Article 2.1, this will be considered again.

Thus there exist within the category personal data, the following subdivisions: *Directly identifying personal data versus indirectly identifying personal data*. It is clear that within the category of personal data, the directly identifying data is more precarious than the indirectly identifying data from the standpoint of privacy, particularly if guarantees have been given that the researcher will not try to determine the identity of the data subject anyway.

#### *Coded versus not coded data*

Coded means that a unique code has been added to the data in order to give the data subjects a unique identity. Such a code can, for example, consist of an encoded version of name, address, sex and date of birth. In order to be able to call this coded data, it is essential that the key is not in the hands of the researcher or someone under his authority. In this sense coding and the concept of coded data also differ from the "meaningless administration number" which will be discussed later (Article 7.1). Such a meaningless administration number is often called a code by the researcher but that is not the case in the sense of this Code. In order to speak of coding, it is essential that the researcher does not have any authority over the key and therefore does not have access to it. As a

rule the key to the code will be in the hands of the supplier of the data. One can also choose an independent third party, such as a Comprehensive Cancer Centre. In other fields, one speaks of a “trusted third party” but this construction does not seem to have become accepted in scientific research.

One can also differentiate between “one-way coding” and “two-way coding”. “One-way coded” data are directly identifying data which have been converted into a code number, but it is of course not possible to determine the identity of the data subject from the encoded data. This is possible with “two-way coded” data, although only by those who have access to the code key. Within the structure of this Code of Conduct this may not be the researcher. From the definition of coded (p) it is clear that it refers to “two-way coded”. In the case of “one-way coded” data, there is not a special privacy problem. After all the code number known to the researcher cannot be used by the researcher – and also not by the supplier - to determine the identity of the data subject. “One-way coded” data does not therefore add anything from the standpoint of privacy to the previously described terms “anonymous”, “directly identifying” and “indirectly identifying”.

Coding can offer enormous advantages for the investigation. In this way data from various sources or successive data from one source can be combined without the change of administrative multiples. Furthermore should it become necessary, additional data on the data subject can be requested at a later stage. Thus the course of a certain condition can be investigated prospectively. Of course in order to realize this advantage the supplier must be able and willing to work with coding.

From the standpoint of the protection of the personal life style, this coding also offers advantages. The most important advantage is that the researcher no longer needs to use certain identifying data in order to achieve the advantages mentioned above. One can therefore work with a less sensitive level of data, namely the indirectly identifying data. In addition as a result of this system of coding, the researcher is not tempted to try to identify the data subject himself

should more data be needed for the investigation. In the eyes of the researchers this is probably a hypothetical situation but for the establishment of the regulations it definitely plays a role. “Two-way coding” can ensure that data is not used for the purpose of identification by the researcher.

In addition to advantages two-way coding also has disadvantages from the standpoint of privacy. In fact so many data could be collected about one person that “anonymous” is no longer anonymous and “indirectly identifying” becomes directly identifying. The fact that in diverse sections of this Code it is forbidden to determine the identity of the data subject makes this impossible in the legal sense. Together with the other guarantees, this also means that it is practically impossible, as long as the controller can demonstrate that there is sufficient supervision in this respect. In a special case it is possible that a researcher will acquire certain information about a certain specific person that could be of significant importance for his future health. The question then arises whether he or she should be told, which in the event of two-way coding would in principle be possible for the supplier of the data.

As indicated in the above, “coded data” are sometimes anonymous and sometimes indirectly identifying. Which type depends partly on the circumstances, such as the means that are available to the processor and the effort that it will cost him to determine the identity of a certain natural individual. The category “coded directly identifying data” is in theory possible but for these regulations it is not of practical importance. Coding does not change the fact that this subgroup already falls in the strictest category. In addition the purpose of coding is in fact to prevent the use of directly identifiable data.

Therefore coding is in practice only important for indirectly identifiable data. The researcher can under certain circumstances profit from a milder regimen than that applicable for personal data in general. See also chapter 5.

The concept “database” (q) is clear in itself. It is necessary because as a rule databases are supplied and not several “loose” data.

### *Section r*

In a number of cases permission of the medical ethical review committee is needed in order to be allowed to process data for a specific investigation. This can be a committee which is acknowledged as a review committee by the CCMO in the sense of the WMO but it need not be. One sees a certain concentration of such committees, certainly in the larger institutions where they are overburdened. Other test criteria for non-WMO research have also been established. This Code of Conduct does not stand in the way of this goal. The committee must however assume that the testing of such research is part of their field of activity and must therefore also be qualified for this purpose. For qualification the requirements given by WMO can be applied accordingly.<sup>2</sup>

---

<sup>2</sup> Not all disciplines required by or chosen on the basis of the WMO to participate in a recognized review committee are needed for evaluation of the relevant investigation. On the other hand, it is desirable to change the composition of the committee for evaluation of the relevant investigation to include at least one epidemiologist.

## Chapter 2 General Aspects

Of all articles, Article 2.1 is crucial. This was already mentioned in the section on definitions. Without this framework all data within the organization of the researcher could be considered as one entity and it probably would never be possible to have anonymous data at the level of the researcher.

The basic principle is that within one organization the conditions established between care providers and researchers and between researchers mutually for supplying databases to one another must be the same as those applicable for an external data supplier. Or, even better, formulated the other way around, the conditions that an external data supplier establishes to protect the privacy of the individual data subject also apply for the supply of (databases with) data within one organization. Only in that way can one be certain that a researcher indeed has anonymous data for an investigation for which the data are supposed to be anonymous when the researcher works within a large organization where there are many databases with data present. If all of the data of that organization were thrown together into one pile, one could never speak of anonymous or indirectly identifying data at the level of the researcher.

In order to make this basic principle operational, the controller – depending upon the organization – must take a large number of measures. They consist of a group of technical and organizational measures. Technical measures are, for example, “firewalls” between databases and access to databases only by means of access codes. Organizational measures are, for example, limited distribution of these access codes and supervision of compliance.

Article 2.2 is to a large extent self-evident. It means that the Code of Conduct does not replace the above-mentioned laws. Furthermore the researcher may assume that by keeping to the Code of Conduct he will never come into conflict with the

above-mentioned legislation. This Code of Conduct is after all the practical elaboration of said legislation.

Article 2.3 is also self-evident. In part it is a repetition of that which applies at the level of the controller. The researcher may assume that the one who provides the data does so in accordance with the current regulations of the WBP and the WGBO (“legitimately”). If he has valid reasons for doubting this, then he should not request the data.

Precaution with respect to the collection, storage and use of data does not mean only general organisational control. The researcher must also take the necessary technical measures against unauthorized inspection, such as locking cabinets, the use of passwords for access to databases, etc. In the research protocol, there should be a description of the steps taken.

From Article 2.4 it can be seen that the form of investigation which interferes the least with the privacy of the data subject is to be preferred. This is an elaboration of WBP Article 11, paragraph 1. When expressed in the terminology of this Code of Conduct and in ascending order of “privacy sensitivity”, the following list can be made: anonymous and not coded; anonymous and coded, indirectly identifying and not coded, indirectly identifying and coded, and directly identifying. For each step higher than anonymous and not coded, good motivation resulting from the design of the investigation must always be given.

Article 2.5 contains a regulation for the situation in which supporting personnel are active as assistant, secretary, intern, etc. The researcher has a controlling task here. This article is an elaboration of WBP Article 12.

Supporting personnel in health care are subject to a derived professional confidentiality when processing personal data. Personal data which become available for an investigation may only be processed by the researchers listed in the protocol. This does not mean that a secretary may not write letters or type a

research report. For them too professional confidentiality also applies, in accordance with WBP Article 12, paragraph 2.

Article 2.6 lays down the contents of the protocol. In this protocol the scientific and privacy aspects of the investigation are described. The concrete safety measures must be specified in the protocol. This would include regulations for use of equipment, authorisation, procedures, etc. Probably one can make use of the general procedures applicable within the organisation (standard operating procedures, SOP's).

Sometimes it will be necessary to change the protocol during the investigation. During the course of an investigation, for example, researchers may leave or others may be recruited. This is acceptable, as long as it is recorded in the protocol. If the total number of individuals with authorized access remains the same, then this can be considered a change of minor significance. One may not change the protocol so drastically that an investigation is created which cannot be considered to have the consent of the data subjects.

Article 2.7 can be seen as an elaboration of Articles 2.2 and 2.3 of the Code of Conduct. Data subjects must be aware of their rights in general. The researcher, who often will never see or know the data subjects, cannot take care of this himself. He must however ascertain that the organization or care provider has taken the appropriate steps. If this is not the case, he would only be allowed to receive and use anonymous not coded data.

Article 2.8 describes the precautionary regulations which are in common usage in practice. Data collected for use in research may only be used for research purposes. This does not go so far as to say that data collected for a certain investigation may only be used for that investigation. However for the new investigation the regulations of this Code also apply. If the data are personal data, then the data subject will in principle have to give his consent for this new

investigation or his previous consent must encompass this new investigation, unless one of the exceptions given in Chapter 5 and Chapter 6 applies.

Article 2.9 refers to other provisions of this Code for the storage of data after the investigation. Data that have been collected for a specific investigation need not as a rule subsequently be destroyed after the investigation. Sometimes however this is the case. When and under which circumstances longer storage is permissible is dependent on the type of data and is specifically particular described in article 5.5 and chapter 7.

In Article 2.10, a principle is described that has already been discussed, for example in the regulations that apply for the controller. Data are collected for use in a specific investigation. If these data are supplied to another researcher, this other researcher must be considered a third party and the use of these data for another investigation must be evaluated once again according to the regulations of this Code of Conduct. Within this context one must realize that “the researcher” is defined as the one who is responsible for the investigation. This regulation does not of course apply for those who work together with this researcher in the execution of a certain investigation and in fact are often also researchers.

Article 2.11 covers the situation in which the care provider wants to carry out research using data on his own patients. Previously it was assumed that there was no reason to prevent the use by a care provider of data on his own patients for research. Relatively often this involves quality of care-like questions. From the point of view of the WGBO there is no question here of supply to a third party. The principle of combined aim or “compatible use” also does not prevent such use for scientific research, since it is continuously assumed that scientific research for health care is also one of the aims for which a care provider - within the framework of patient care - can and sometimes even must use collected data. The most recent version of the Hippocratic Oath for Dutch physicians (KNMG, 2003) states in addition “I shall promote my own medical knowledge as well as

that of others". On the other hand there is so-called "special (personal) data" in the sense of Article 16-23 WBP for which a stricter form of combined aim applies. In order to end all further discussion a regulation has now been included which states that in the event of such use by the care provider, the system of "no objection" applies.

This (no) objection system must in general be defined at the institutional level (see Article 2.6). It is much easier to explain that this also applies for research carried out by the care provider himself. It does justice to those who do not have sufficient confidence in the investigation and want to protest against it, although by making use of the health care provided they also profit from previous scientific research and this care is considered to be increasingly "evidenced-based".

According to Article 2.12, the processing of personal data in an investigation implies that the evaluation by the medical-ethical review committee must have been positive. In other cases the researcher must continuously ask himself whether the proposed investigation involves such privacy aspects that it must first be reviewed by a medical-ethical review committee. The nature of this committee has already been considered in the section on Definition of Terms. The responsibility to judge whether evaluation beforehand is required lies in the first instance with the researcher. For example, whether the results of an investigation may be expected to be of special significance for a specific group of the population. Should he fail in this respect, he can later be called accountable, for example via the complaints committee or eventually the peer disciplinary board.

The phrase "taking into account that which is specified elsewhere" means that a researcher cannot (by making use of this Code of Conduct) ignore the regulations of the organization for which he works or where the investigation is carried out. Such regulations can for example state that every health investigation must be evaluated by the review committee active there.

Article 2.13 describes the notification of the processing of personal data at the CBP (the Data Protection Authority). In first instance every systematic processing of personal data for the purpose of research must be reported. There

is however one exception. This exception is in essence that the processing of indirectly identifying data for a certain investigation need not be reported as long as these data are not coded. Also if one has communication data on the data subjects in one's possession for a short time, the investigation need not be reported. At the same time one must satisfy a number of precautionary requirements. The communication database and the research database must be stored separately. Six months after the data have been obtained from the data subject, the communication data must be destroyed. An exception can be made for data on sex, city, and year of birth. The destruction of the communication database does not mean encoding this data. In that case the investigation would still have to be reported.

Notification is possible without much fuss via the electronic route by completing the notification program at the site of CBP at [www.cbpweb.nl](http://www.cbpweb.nl).

### **Chapter 3: The use of anonymous data**

Use of anonymous data is in principle not a problem from the standpoint of privacy. Neither the WGBO nor the WBP contain regulations for the use of anonymous data.

The Code establishes one important but also evident prerequisite. In Article 3.2 it is stated that it is "forbidden to create links which could identify the subject". It is forbidden to manipulate anonymous data such that identifying data are created. The aim of this regulation is evident. It is especially important if one uses non-identifying data which are also coded. If several of these databases are joined, which in principle is possible via the coding, one must make sure that the new database cannot be considered to be indirectly identifying data. In that case namely the stricter requirements from the next chapters must be satisfied.

According to Article 3.4, these data may be processed and therefore also stored for as long as it can be expected within reason that they can be useful for research. This need not be for the same or a comparable investigation.

#### **Chapter 4: The use of personal data**

This chapter contains the main regulations for the processing of personal data. They are based on a system of consent. There are two exceptions to the main regulations. In some cases it will not be feasible to request consent. Then one may use indirectly identifiable personal data (whether coded or not) under certain conditions. This is described in Chapter 5. When it is not possible to request consent and it is also not possible to encode the data, then the researcher may still process – whether briefly or not – the data, although under certain very strict conditions. This is discussed in Chapter 6.

But now, first the main regulation.

Personal data may in the first instance only be processed for health research after the data subject has given his consent (WBP, Article 8 and Article 23; WBGO, Paragraph 1; Article 7:457 BW). The request for consent must include information relevant for the data subject. The Code of Conduct states what that information should be in general. It is not necessary to go into the details of the investigation.

The WBGO leaves the form of the consent open. Written consent is not a requirement. As a rule, verbal consent satisfies the law. The consent must however be explicit, not implied. If the data are extremely sensitive or if the investigation is expected to last longer than the treatment relationship with the data subject, then written consent is to be preferred. The same applies whenever a (new) research question arises after the end of treatment.

The consent can be revoked. In that case the care provider must inform the researcher to whom he supplied the data. The researcher must then destroy the

data pertaining to that patient/client. Or the data must be rendered anonymous. Revoking consent only makes sense when the personal data can still be used in an investigation. If the investigation has already been completed then revoking consent will no longer have any consequences.

In Article 4.2, the regulations for the representation of incompetent patients and minors in the WGBO are presented. If the data are supplied by a care provider, then it is up to the care supplier to ensure that the authorized representative has given proxy consent.

The regulations for representation in the WGBO are fairly complex. In summary they can be stated as follows:

- The adult incompetent patient is represented either by a representative appointed by a judge or by a representative appointed by the patient or by the patient's partner or by the patient's parents, brother or sister. The order of representation is mandatory with the exception of the phrase beginning with "patient's parents".
- Minors younger than 12 years are represented by both parents, insofar as they exert parental control, or a guardian.
- For minors between 12 and 16 years, as long as they are competent, a double system of consent applies for treatment in principle. Under certain circumstances however the consent of the child alone is sufficient. The parents have the right to view the medical records of their child, as long as this is not against the best interests of the child (Article 7; 457, third paragraph).

According to the WBP, minors up to 16 years of age are represented by the parents, as long as they exert parental control. Since the WGBO is a "special law" one may assume that double consent also applies in this case. In exceptional situations only the consent of the child should be sufficient. This is the case when the care provider refuses to allow the parents access to the records because this access would be against the

best interests of the child. For example, if the child is treated without the consent of the parents.

- From 16 years of age, the child - if competent – has independent authority over his treatment according to both the WBP and the WGBO. Then only the young person needs to give his consent.

The second sentence of Article 4.2 describes the situation (which however is exceedingly rare in practice) in which a youngster whose data are used in an investigation on the basis of consent given by the parents subsequently revokes this consent when he reaches the age when he may make this decision.

As a rule the researcher will obtain exposure-sensitive data from a third party. Article 4.3 states that the researcher must be aware of the fact that this third party has satisfied that stated in Article 4.1. Furthermore it is sufficient that the supplier declares this explicitly. The researcher himself need not run a check on the supplier.

Article 4.4 is a regulation which once again emphasizes the importance of not doing anything more with the data than originally specified. The second sentence is a variation of the regulation that it is forbidden to link anonymous data and is included for the sake of completeness.

## **Chapter 5: The use of indirectly identifying, coded or not coded, personal data without the consent of the data subject**

This chapter focuses on the situation in which the researcher wants to process personal data but it is not feasible to ask the data subject for his consent. In such cases, either many patients will be the data subjects or the data were obtained from patients who were treated a long time ago. It would take a disproportionate amount of time and effort to discover the actual addresses of these patients in order to request their consent.

In such cases the investigation may be carried out as long as the prerequisites stated in Article 5.1 are also met. This Article is based on Article 7; 458, first section, paragraph b and the second paragraph of 7:458 of the WGBO. This Article is a further specification of Article 23 of the WBP.

The most important prerequisites are that the personal data are free of directly identifying characteristics and that the data subjects have expressed no objection to such use, as far as is known. For purposes of the methodology of the investigation, for example if the data subject was followed for a longer period or data from various sources have been combined, the data can be encoded such that the unique data on the data subject can be included.

The research protocol plays a decisive role in demonstrating that the situation defined in 5.1 applies. For the no objection system, see Article 2.7. The researcher need not visit the care provider in order to check whether the no objection system has functioned. He is obligated to ask the care provider explicitly and to obtain a positive answer. The explicit manifestation of the public interest is partly inspired by Article 30 of the Decree on the Exemption from notification of the WBP. In that Decree, organizations for scientific research or statistics are mentioned specifically. Being able to publish the results of an investigation is by definition in the public interest of an “open society” (following Popper), even though the concrete advantages of the results may possibly not be evident in the short-term perspective.

It should be emphasized that this is not the only reason that coded personal data can be processed. Even when the request for consent is possible, it must be determined whether indirectly identifying and then coded personal data can be considered sufficient. After all, from the standpoint of privacy, the processing of coded personal data is less precarious than the processing of directly identifying personal data. But that processing of coded personal data cannot be based on the exception to the consent principle described in this chapter. If it cannot be claimed that the request for consent could not be made within reason or was not possible (as described in the next chapter), said consent must be present when one works with indirectly identifying coded or not coded personal data.

Articles 5.2 and 5.3 describe the manner in which the – coded or not coded – indirectly identifying data are obtained and are clear. Article 5.2 does not require an official agreement with the supplier but the researcher and the supplier must agree to the safety precautions in writing.

Article 5.2 regulates the rights and obligations of the supplier/care provider and the researcher as well as the (technical) manner of the transfer of data. The researcher must satisfy the requirements of the research protocol (Article 2.6), including also the regulations for access and protection of the data as well as the storage deadline. The key to the coded data remains of course part of the professional confidentiality of the supplier/care provider.

It is forbidden to manipulate coded data such that directly identifying data are created. The agreement between the researcher and the care provider, which regulates the provision of data (also in the technical sense), must in fact guarantee that the researcher himself cannot determine the identity of the subject. This also means that the aggregation level at which the researcher stores the data provided must be such that identification is not possible. In addition, the method by which double entries are avoided (in the event of multiple suppliers) must be a guarantee that the researcher cannot deduce the identity of

the subject. In Article 5.4 the fact that linking is forbidden is once again stated in so many words.

If the researcher wants new coded data about the data subjects in his investigation, they must be obtained from a supplier (Article 5.3). This sometimes occurs because the researcher asks the supplier for supplementary data about one or more data subjects with coded data. Sometimes the research protocol will contain a provision that, according to the schedule in the protocol, databases with coded data will be supplied to the researcher so that an already existing database can be enriched.

At all times, there must be a guarantee that linking at the individual level remains forbidden. The indirectly identifying data may not now become directly identifying.

The previously described prohibition of linking in 5.4 has already been considered in relation to anonymous data. The significance is evident. Indirectly identifying data can in theory be used to derive an identity. If this were not the case, then the data would be anonymous. Even if they can in theory be used to derive the identity, this should never be done in practice (in the unlikely event that a researcher would think of this) This applies of course also if the indirectly identifying data are coded.

According to this chapter the coded or not coded indirectly identifying data are collected for one specific investigation. They may only be used and stored specifically for that

investigation. The predicted period of storage ends after the results are published and it is no longer reasonable that questions will be asked in the literature on the basis of analyses which would make renewed evaluation of the data necessary. As a rule this period can be set at five years.

During that period it is possible that the data will be found to be useful for another investigation. In principle this is possible. In that case however the same applies

here: because the data are personal data, although a special form of it, the data subject must have given consent or one must apply the regulations given in this chapter to the new investigation.

## **Chapter 6: The use of personal data without consent of the data subject**

In this chapter the second exception to the system of consent for the processing of personal data will be considered. This is an extrapolation of Article 7:458, section 1 paragraph a and paragraph 2 of 7:458 WGBO in connection with Article 23, second paragraph WBP.

This is a regulation designed expressly as a safety net. The exceptions are valid whenever the investigation cannot be carried out via the route of consent or via the use of coded or not coded indirectly identifying data without objection. Sometimes a situation arises in which the request for consent is not really possible but one still needs personal data. These are almost always situations in which the data subject cannot or does not want to answer the request for consent or in which the question cannot be asked. The latter is due to the nature of the request for consent and sometimes the circumstances of the person who must respond to the question.

This can occur in the situations listed in Article 6.1. In that case too the type of personal data must be chosen that offers the most protection of privacy. Preferably, therefore, indirectly identifying data. But in some cases, which will be discussed explicitly in this chapter, one cannot avoid using directly identifying data used. That is why the exception described in this chapter goes farther than that defined in the previous chapter, in which only indirectly identifying data could be used. The prerequisites are also much stricter.

The first situation (Article 6.1, sub a) refers to the mental burden that the request for consent might cause the data subject: this question can in some cases represent such a heavy burden that the request for consent must be considered

irresponsible. Consider for example the unexpected confrontation with previously received (sensitive) information which is not in the interests of the data subject. Mental suffering must not be assumed too quickly, that is why a connection is established between the nature/severity of the condition, the time which has passed since the last treatment contact and the time when the need for data became apparent. Whether such a situation occurs must be determined in the first instance by the medical-ethical review committee. Subsequently the care provider who supplies the data must concur with their evaluation. The latter has the last word about whether the data can be supplied to the researcher.

The second situation (6.1, paragraph b) is practical in nature. It concerns circumstances beyond the powers of the researcher. The written request should of course be sent to the correct address. Sufficient attempts – within reason – must be made to find the correct address.

The third situation (6.1, paragraph c) occurs when a large group of people would have to be asked to consent while only a much smaller group of people is needed for the investigation. Only the personal data of the smaller group will be used for the investigation. A brief inspection of several data of the larger group is carried out in order to select the smaller group from this group. It is important that the researcher makes this selection and not the care provider in order to avoid “bias” in the selection. Of course the selected group must subsequently be asked for consent to be included in the investigation (see also 6.3, paragraph e). The large group cannot be asked for their consent because this would pose a question for which there is no proper answer and would even lead to many questions and uncertainties. One would have to ask them if they would consent to participate in a certain investigation of a certain condition while they very probably do not have the condition and they probably will not be included in the investigation.

In the fourth situation the investigation is in such a preparatory stage that the request for consent is meaningless. There is as yet no clear-cut hypothesis, actually only an idea which must be converted into a concrete research question.

In order to be allowed to review personal data in these situations, a number of additional prerequisites must be satisfied. In all cases the prerequisites given in Article 6.2 must apply. In addition for the last two situations a number of extra requirements, described in Articles 6.3 and 6.4, apply.

As previously mentioned the presence of one of the situations described in Article 6.1 is not sufficient. Article 6.2 describes the requirements which - no matter what - must be satisfied in order for an appeal on the basis of these exceptions to be successful.

- a. The researcher must substantiate the scientific importance of his actions. He must not only indicate why the prerequisites listed under a have been satisfied but he must also show that without these data the investigation cannot be carried out or has become worthless for methodological reasons. Alternatives must be considered.
- b. This is an elaboration of Article 2.4. All things considered, there are two points of review, once it has been established that within reason a request for consent is not possible. The first is the question of whether it is possible to work with anonymous data or at least to some extent. The second point of review is to ensure that when personal data are used, no or as little directly identifying data as possible will be included. Eventually one could also use coded data here in order to prevent the problem of direct identification.
- c. This prerequisite concerns the lack of a (prior) objection made by the data subject which of course should be known to the care provider.
- d. As a rule this prerequisite will be satisfied as long as everyone works according to the regulations of this Code of Conduct, especially the regulations given in Chapter 2. Chapter 7 is also important in this respect, namely the separation of the database with directly identifying data from the research database.

Articles 6.3 and 6.4 consider in more detail the prerequisites for the two situations in which a researcher requests that a care provider grant incidental short-term access to personal data once. The two Articles are clear in themselves. Ultimately the treating physician must decide whether the circumstances described here are such that he or she can grant the requested access in view of the sensitivity of the data that have been entrusted to him or her by the patient. The access takes place in his/her work space and under his/her responsibility. In 6.4 (being able to complete the investigation protocol) it is not considered worthwhile to present this situation ahead of time to the review committee. The requirements described are already highly restrictive whereas in the event of a lack of a protocol, the review committee will have difficulty pronouncing judgement.

## **Chapter 7: Special regulations for the processing of directly identifying personal data.**

The first Article of this chapter contains a safety precaution for the use of these data by the researcher. This speaks for itself and is already common usage by most researchers. The internal coding does not transform these data to coded personal data or anonymous data. As mentioned in the definition of terms, it is necessary for this purpose that the code key does not fall within the authority of the researcher.

Article 7.2 too contains extra safety precautions. At the same time it answers the question of which data may and may not be stored after the investigation. The communication database is tied to the aim of it and should be destroyed as soon as it is no longer needed for this investigation. For the data which are subsequently left over, the connection to the goal is less strict. Storage for the sake of storage is not acceptable, unless there is a reasonable chance that the data will be needed for another investigation. If indirectly identifying personal data are involved, which have been obtained for a specific investigation according to the criteria given in Chapter 5, then according to Article 5.5 they may in principle only be stored for that investigation. The exception to the principle of consent by means of which they could be obtained applied for that specific investigation. However a new investigation could make use of the same data after they have been stored as long as the new investigation satisfies the requirements of Chapter 5. This will have to be evaluated once again by the medical-ethical review committee.

In summary, the following regulations apply for the storage of data:<sup>3</sup>

- Anonymous data: no specific period
- A research database with indirectly identifying personal data (coded or not coded), according to Chapter 5: as long as reasonably can be expected

---

<sup>3</sup> Article 7:454 BW (WGBO) specifies the period of storage for medical data by care providers and does not therefore refer to the storage of data for scientific purposes by researchers.

that it can be used for the relevant investigation. Re-use is however possible, again if the circumstances occur as given in Chapter 5.

- A research database with personal data in which directly identifying data are included: as long as reasonably can be expected that they can be used for the relevant investigation.

The significance of the phrase “as long as reasonably can be expected that they can used for the relevant investigation” has already been discussed in Article 5.5.



## Chapter 8: Complaints

Data subjects must be able to lodge a complaint. On the basis of Article 2.6 they have already been informed in a general sense about the existence of a complaints committee at the institution. If asked the researcher himself must inform the data subjects properly about ways to lodge a complaint. It is part of the responsibility of the researcher to make sure that there is a good procedure for complaints about health research. Such a procedure for complaints should satisfy the minimum requirements of the Law on the right to lodge a complaint for clients of the health care sector or the model for the regulation of complaints of the KNMG. Thus the guarantee must be given that the researcher will not participate in the decision making about a complaint and that the complainant will be informed as soon as possible after judgement whether measures will be taken and if so, which ones. The FMWV has set up a complaint committee which satisfies these requirements in a corresponding manner. If the organization where the researcher works does not have its own regulations and states this preference, complaints can be referred to this committee. The patients/clients involved can however also choose another (legal) route in order to bring the case about the investigation and the manner in which his data were used before the courts.