

Handling of Your Medical Data

This fact sheet is intended for the *data subject*, i.e. the individual whose personal data is being used.

THIS FACT SHEET WILL ANSWER THE FOLLOWING QUESTIONS:

Who is responsible for my medical data?

What information is included in my file?

How long is data kept?

How is my medical data protected?

What conditions apply to the use of medical data for scientific research?

What do I do if I would like to find out more or have a complaint?

You may want to know if your specialist or the hospital is responsible for your medical file. Or perhaps you wonder whether the personal case notes made by your psychiatrist also form part of your medical file. Or maybe your GP sends data to the pharmacy by e-mail and you wonder if this is allowed.

The relationship between you and your care provider is regulated by law. The Wet op de geneeskundige behandelingsovereenkomst (Wgbo) [Medical Treatment Contracts Act] lays down the rights and obligations of care providers and patients. In addition to the Wgbo the Wet bescherming persoonsgegevens (Wbp) [Dutch Data Protection Act], the Wet bijzondere opnemingen in psychiatrische ziekenhuizen (Wbopz) [Psychiatric Hospitals (Compulsory Admissions) Act] and the Wet op de jeugdzorg (Youth Care Act) also contain stipulations relating to medical data.

Responsibility for your medical file

According to the Wbp the 'data controller' is the party that determines the objective and methods for processing personal data. In an institution, the Executive Board or Management Board is often the data controller within the meaning of the Wbp. In other words, they determine what happens to the data held in an institution.

In addition to the Wbp the Wgbo is also relevant. The Wgbo applies specifically to care providers. Although a care provider who is employed by an institution is not a data controller within the meaning of the Wbp, pursuant to the Wgbo he is, however, responsible for the contents of his patients' medical files. He is also responsible for the provision of your medical data to others, either by him or on his behalf. Further information about the forwarding or non-forwarding of your medical data can be found in the fact sheet entitled *Confidentiality of your medical data* [Geheimhouding van uw medische gegevens]. In addition, the care provider is responsible for deciding whether to comply with your request in respect of access, erasure or supplementation of your medical data. Further information about your rights can be found in the fact sheet entitled *Your rights as a patient* [Uw rechten als patiënt].

The responsibility for your medical file, therefore, rests both with the Executive Board or Management Board of an institution and with individual care providers.

Contents of your medical file

A care provider has a duty to maintain a separate file for each patient. A file is all of the data a care provider records about a patient. Exactly what data must be included in the file differs depending on the treatment and the medical discipline in question. The individual care provider can determine what data is included in the file, but this is also dependent on statutory stipulations or regulations, such as the Wbopz and the associated Besluit Patiëntendossier Bopz [Bopz Patient File Decree], which may apply.

In addition to the obligation to maintain a patient file, the care provider also has an information obligation. This means that he must keep you informed in language (verbal or written) that is understandable to a layman.

This concerns information about your illness or condition, the nature of the proposed treatment, the examination, alternative treatment options, the consequences or potential risks of the treatment or examination and about the prescribed medication and any potential side effects.

The file must in any case contain the basic details. These are, among others, the findings of physical and psychiatric examinations, the diagnosis, treatment that has been initiated, progress of the treatment, anaesthetic and surgical procedure reports, important laboratory results, referral and discharge letters, x-rays, nursing reports, notes of any discussions and findings of previous care providers or experts who were consulted. Any information and statements provided to you must also be included in the file.

Personal case notes made by the care provider do not belong in the medical file. Personal case notes are impressions, presumptions and questions. They serve as a reminder for the care provider and are not to be shared among medical colleagues. As soon as the care provider shares personal case notes with his colleagues by including them in your file, it is then *your* rights - such as the right of access or erasure - which are applicable. In general the handling of any complaints and liability issues are not included in the medical file either. An independent Complaints Committee and the Management Board will create a separate file for such issues.

The Wbopz and the Besluit Patiëntendossier Bopz stipulate the minimum data to be included in the file of a psychiatric patient who has been involuntarily admitted. This may be the treatment plan, the reason why no agreement was reached about the treatment plan, the restrictions to the patient's freedom of movement, any copies of court decisions that have been received, the admission and discharge details and any reports issued in the context of a hospital order.

Retention period of your medical file

The general retention period for medical files is 15 years. This change is an interim measure in anticipation of the decision to extend the retention period to at least 30 years as a result of advice issued by the Gezondheidsraad [Health Council]. At the end of the retention period the file must be destroyed. There are some exceptions to the general 15-year retention period, namely in the case of:

- good care provider practices *or*
- statutory obligation *or*
- patient's request *or*
- anonymous details *or*
- the interest of others.

Good care provider practices

Your medical data may be retained longer if this is a reasonable consequence of the care provided by a good care provider. Your GP can also hold on to your medical data for more than 15 years in the context of the continuity of your care.

Statutory obligation

A statutory retention period of 5 years after the end of the involuntary admission applies to the files of psychiatric patients who were admitted under a hospital order. For psychiatric patients who were admitted voluntarily the general retention period of 15 years does apply. The Archiefwet [Public Records Act] applies to certain data in university hospitals. Documents such as the surgical procedure report and the discharge letter must be kept for 115 years. Data relating to a medical check-up must be kept as long as needed for the objective for which the check-up was performed. This will usually be less than 15 years.

Patient's request

You can ask a care provider to keep certain medical data for more than 15 years. Alternatively, you can ask for your data to be erased, which makes the retention period less than 15 years. However, pursuant to the Wbopz a patient cannot request erasure of his data before the statutory retention period has expired.

Anonymous details

If your care provider removes any personal information from the data, making it anonymous, the data can be kept longer than 15 years. Data is anonymous if it cannot be related to a person, or if it can only be related to a person with disproportionate effort. Deletion of the name is not always sufficient. The retention of anonymous data is mainly relevant to scientific research.

The interest of others

In the case of hereditary conditions a care provider can keep data longer than the general retention period in the interest of your children. Another example is a situation whereby your care provider may need the data in the context of legal proceedings you have initiated against him.

Security of your medical file

The Wbp imposes an obligation on the data controller concerning the security of the processing of personal data. Suitable technical and organisational measures must be taken to prevent the loss or unlawful processing of data. The protection of personal data is the responsibility of the responsible party in question. The responsible party must take the risks inherent in the processing of data into account.

In addition to the Wbp the Dutch standard for data protection, NEN 7510, is a relevant directive for the care sector. NEN 7510 provides guidelines and starting points to determine, implement and maintain data security measures for care institutions. At present there is no statutory requirement for care institutions to comply with the standard. It is expected that this will be the case in the course of 2008, as a result of the introduction of the Citizen's Service Number [Burgerservicenummer] in the care sector.

Comprehensive information about the protection of data can be found in the Dutch DPA study entitled *The Security of Personal Data* [Beveiliging van persoonsgegevens]. This report assumes three levels of protection, subdivided into exclusivity classes. Because of the use of special data the highest level of protection is required. Some requirements for the protection of medical data are:

- the implementation of access control in respect of electronic files;
- the encryption (application of encryption techniques) of health-related data on the Internet;
- the storing of information carriers, such as paper files and computer disks, in a burglary-resistant environment;
- outsourcing of data to another organisation only if this organisation has implemented the required security measures;
- deletion of data so that reconstruction of the original data is no longer possible.

The aforementioned study lists a number of security regulations. It is important that clear agreements are made within an organisation in respect of the measures to be implemented. These agreements must also be documented and must be known to the employees. Following are two examples of security measures in relation to the sending of medical data.

Faxing of medical data

In many cases, faxing medical data will not be sufficiently secure and must therefore, in principle, be avoided. Whether this method is secure enough depends on a number of factors. On the one hand, the line used to send information by fax does not generally have additional security. On the other hand, the security of the data transmission is linked to the question whether it concerns a personal fax aimed at one recipient or a shared fax addressed to a number of persons. In addition it is important that the person who is the recipient of the fax is aware of the time it is being sent. If this is not the case there is a risk that the fax may remain in the fax machine (unsupervised) for some time. This makes it possible for persons other than the intended recipient to read the contents of the fax

E-mailing of medical data

Sufficient security measures must also be implemented in respect of the e-mailing of medical data such as, in this context, the formulation of a user guideline and the implementation of anti-virus and anti-spam software.

In addition, the storage facility for e-mails must be secured against unauthorised access and medical data must be encrypted before being sent. It is also useful to implement logging facilities, which make it possible to trace the cause of any infringements so that measures can be put in place to prevent a repeat occurrence.

Use of your medical data for scientific research

The main rule for the use of your medical data for scientific research and statistical purposes is that you must have given permission for such usage. There are two exceptions to this main rule. Your permission is not required if:

- it is not reasonably possible to request your permission and the research is covered by sufficient guarantees to ensure that your personal privacy is not disproportionately infringed *or*
- in view of the nature and objective of the research it cannot reasonably be expected that your permission is requested and the care provider has taken care that the data is provided in such a format that it is not reasonably possible to trace back the information to individual natural persons.

When applying either of these two exceptions the following conditions must also be met:

- the research must serve the general interest *and*
- the research cannot be completed without the data in question *and*
- you have not specifically objected against your data being made available.

If your data is being supplied for scientific research or statistical purposes the care provider must include a note to that effect in your medical file.

The further definition of the aforementioned regulations can be found in the *Goed Gedrag* [Appropriate Conduct] code of the Federatie van Medisch Wetenschappelijke Verenigingen in Nederland [Federation of Medical Scientific Associations in the Netherlands] (www.fmvv.nl), in the *Gedragscode voor verwerking van persoonsgegevens bij onderzoek en statistiek* [Code of conduct for the processing of personal data for research and statistical purposes] and the Dutch DPA report entitled *Privacy bij wetenschappelijk onderzoek en statistiek* [Privacy protection in scientific research and statistics]. The first code of conduct applies to medical data that is subject to professional secrecy and the second code of conduct applies to data that is not subject to professional secrecy.

In the case of questions or complaints

If you feel that your care provider is not handling your medical data correctly, there are a number of options open to you. As an initial step you should discuss your case with your care provider. If you are not satisfied about the outcome of this meeting or if you do not wish to discuss the matter with your care provider, you can take a number of further steps.

Every care provider is obliged to establish a complaints commission. In simple and clear cases the complaint can also be handled by a complaints functionary or confidential representative. You can submit complaints about physicians, dentists, obstetricians/midwives, pharmacists, nurses, physiotherapists, health care psychologists and psychotherapists to a regional Tuchtcollege voor de gezondheidszorg [Disciplinary Committee for the Healthcare Sector]. Alternatively, you can submit a complaint to the Officier van Justitie [Public Prosecutor]. For advice and support you can contact the Zorgbelangorganisatie in your region via www.zorgbelang-nederland.nl or by telephone on number 0900 2437070. [There are 13 care associations in the Netherlands, each active in its own region. They act on behalf of those who need care in the region, give information and try to achieve the highest quality in care. Zorgbelang Nederland is the sector organization of the regional care associations.] You can also submit any questions or complaints about the handling of your medical data to the Dutch DPA. Further information about the Dutch DPA complaints procedure is available in the fact sheet entitled *Your complaint and the Dutch DPA* [Uw klacht en het CBP].