

Privacy regulations Mohs Clinics

Author: H. Bruinsma
Administrator: A. van den Wijngaard
Judge: A. van den Wijngaard
Date added: September 18th, 2013
Last amended: January 21, 2020
Expiry date: January 21, 2022
Version: 4.0

PRIVACY REGULATIONS MOHS CLINICS

**Disclaimer: This text has been automatically translated from Dutch.
No rights can be derived from the English text.**

General considerations

These privacy regulations for patients and employees state how Mohs Clinics handles automated and non-automated personal data. The personal data that Mohs Clinics processes mainly concern patient, personal and financial data. Having privacy regulations is part of the accountability that organizations have in accordance with the EU privacy regulations.

Mohs Clinics attaches great importance to the protection of personal data. This not only concerns the information on computers, but also the information on paper and the behavior of employees who handle this information. These regulations apply to both patient and staff data. Mohs Clinics acts with regard to the processing of personal data in accordance with the applicable laws and regulations, including the General Data Protection Regulation, which in any case means that we:

- process personal data in accordance with the purpose for which they were provided.
- collect only those personal data necessary for the purposes for which they are processed.
- have taken appropriate (technical and/or organizational) measures to ensure the security of personal data, see point 5 of these privacy regulations.
- be aware of the rights of patients and employees, respect them and inform patients and employees accordingly.

Mohs Clinics Foundation (CoC 24436123), including Mohs Clinics established in Dordrecht (CoC 24436381), Mohs Clinics established in Amsterdam (CoC 51560151) and Mohs Noord Holland established in Hoorn (CoC 55264611), is responsible for the processing of personal data of patients and employees. The data protection officer is in charge of the privacy policy. He is the contact person for patients and employees in case of questions and/or requests concerning personal data.

Data Protection Officer: Adry van den Wijngaard
Email address: a.vandenwijngaard@mohsklinieken.nl

EMPLOYEES

Personal data	Special data
Name data	copy ID card
Date of birth	If applicable: Medical data
(Mobile) phone number	
E-mail address	
Marital status	
Insurance data	
BSN	
IP address	

PATIENTS

Personal data	Special personal data
Name data	
Date of birth	
(Mobile) phone number	In case of treatment agreement as well:
E-mail address	Medical data medication use
Marital status	Medical data health
Insurance data	Data as doctor/pharmacy
BSN number	

Article 1. General provisions

1. The Board of Mohs Clinics Foundation is responsible for the processing systems used.
2. Personal data will only be processed with the consent of the data subject and/or in view of an obligation under the law such as AVG, WGBO, the BIG Act and the Wvpz.
3. The Board of Mohs Clinics Foundation is responsible for observing the standards set by law.
4. Within Mohs Clinics a packet of measures, protocols etc. as complete as possible is in function These are: Mohs Clinics company regulations, medical specialists company regulations, confidentiality declaration, protocol for computer use, data leakage notification obligation protocol, processing register, privacy regulations, Mohs Clinics privacy declaration and job description of data protection officer.
5. This description is stored in Mohs/General/VMS/organization.

Article 2. Purpose

1. These regulations relate to data processing for both patients and employees of Mohs Clinics.
2. The aim is to give a practical elaboration of the provisions of the GTC and possibly the provisions of other laws such as the WGBO, Wvpz etc.

Article 3. Conditions for lawful processing

1. Personal data shall be processed lawfully, properly and carefully.
2. Personal data shall only be processed insofar as they are sufficient, relevant and not excessive.
3. The Board of Mohs Clinics Foundation is responsible for the proper functioning of the processing of personal data.
4. To comply with our accountability Mohs Clinics keeps records of processing and any data leaks.

Article 4. Appointment of Data Protection Officer

Mohs Clinics has appointed the Managing Director as Data Protection Officer (FG). There is a job description of his responsibilities, tasks and replacement in his absence. See Mohs/General/VMS/staff.

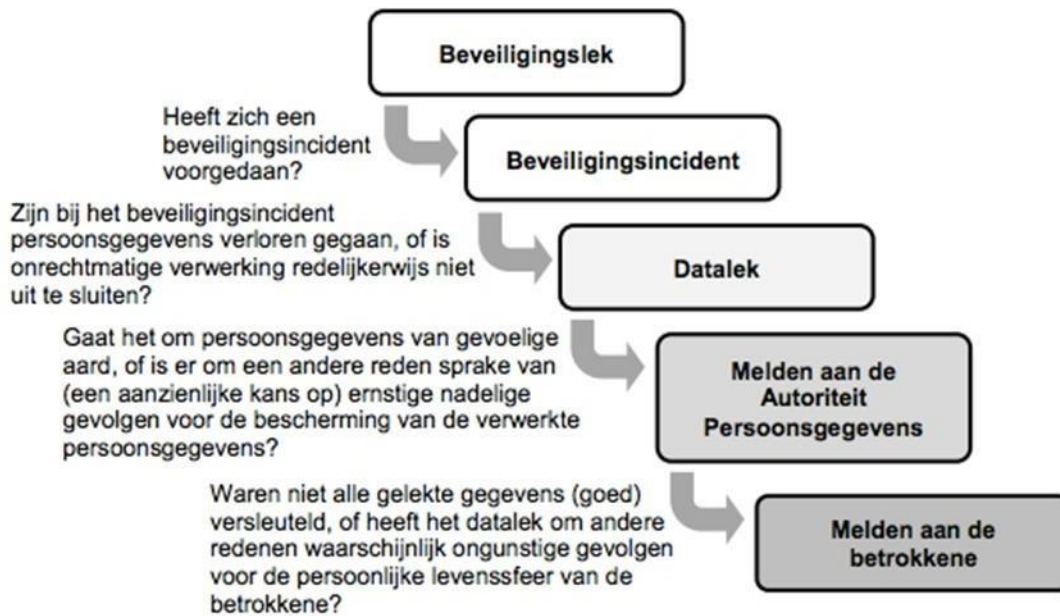
Article 5. Security of personal data

The Board of Mohs Clinics Foundation is responsible for observing the standards set by law. This shall at least include appropriate technical and organizational measures to protect personal data against loss or against any form of unlawful processing.

Measures taken include:

- Patient and staff files are always as up to date as possible.
- Mohs Clinics works with suppliers, with whom a processor agreement has been concluded and agreements have been made about the safe connection and installation of applications/programs.
- Already during the development of products and services privacy enhancing measures are taken and data minimization will be applied (Privacy by Design).
- The standard settings of software systems and the website are set privacy friendly by default (Privacy by Default).
- The software/systems are up-to-date and secured with login encryption, authorizations, encryption and logging.
- A declaration of confidentiality is signed by persons who are not employed by Mohs Clinics but do have temporary access to personal data.
- Password policy (e.g. password consists of at least 8 characters and must be changed after max. 90 days. An account will be blocked after 5 incorrect login attempts)
- USB outputs are blocked.
- For mobile logging in or working from home, we work safely by means of two-stage authorization.
- There is adequate protection against viruses, spam and other external dangers (Managed antivirus 2 way firewall).
- Employees of Mohs Clinics apply a clean desk and clean screen policy. Systems are switched off when leaving the work place.
- Exchange of information, communication between colleagues always takes place securely. E- mailtraffic with patient data from Mohs Clinics is secured (via Edifact). If medical data is sent via the app SILO is used.
- Mohs Clinics uses a protocol for mandatory notification of data breaches.
- The privacy of personal data within Mohs Clinics is a regularly recurring agenda item during work meetings etc.

Article 6. Reporting leak of security by Data Protection Officer



Translation

Has a security incident occurred?	Security incident
Have personal data been lost at the security incident or can illegitimate processing not be reasonably ruled out?	Data leak
Is it about personal data of a sensitive nature or is there for another reason the case of (a considerable chance of) serious disadvantageous consequences for the protection of the processed personal data?	Report to the Authority Personal Data
Were not all leaked data (well) encrypted or has the data leak probably for another reason unfavourable consequences for the privacy for the person concerned?	Report to the person concerned

Article 7. Processing of personal data (insofar as no care data)

1. Personal data may only be processed if one of the following conditions is met:
2. the data subject has given consent to the processing (informed consent for patient data and declaration of consent/withdrawal for staff)
3. processing is necessary for the performance of an (employment) agreement with the data subject, or for actions that are performed for the conclusion of a treatment agreement
4. this is necessary to comply with a legal obligation
5. this is necessary to combat a serious danger to the health of the person concerned
6. this is necessary for the performance of a public law task
7. this is necessary to promote the legitimate interest of the Board of Mohs Clinics or of a third party to whom the information is provided, whereby the interest of the person concerned does not prevail.

Article 8. Specific rules for the processing of health care data

1. Processing of patient data by Mohs Clinics is based on b (execution of medical treatment agreement) and/or a (informed consent). Exceptions are mentioned in paragraphs 2 and 6 of this article, or if provision is necessary for the implementation of a statutory regulation.
2. Without the consent of the person concerned, the Board of Mohs Clinics Foundation may - with due observance of the third paragraph - provide personal data concerning health to:
 - a. care providers, institutions or facilities for health care or social services insofar as necessary for the proper treatment of the person concerned.
 - b. insurers to the extent necessary for the risk to be insured or for the performance of the insurance contract, to the exclusion of paragraph 4 of this Article, and the person concerned has not objected.
3. Personal data shall only be communicated to persons or institutions who are obliged to maintain confidentiality by virtue of their office, profession or legal obligation.
4. In addition to the professional who collected the data, access to the data processing shall be granted only to those directly involved in the performance of the processing agreement, to the extent necessary.
5. The Board of Mohs Clinics Foundation or employees appointed for this purpose also have access.
6. If personal data are rendered anonymous in such a way that they cannot be traced, the Board may decide to provide them for purposes that are compatible with the purpose of the data processing.
7. Personal data concerning a person's religion or belief, race, political affiliation and sexual life may only be processed insofar as this is necessary in addition to the provision of personal data concerning a person's health as referred to in paragraph 2 of this article.
8. Personal data can only be provided for scientific research and statistics without permission if:
 - a. the research is of general interest
 - b. the processing is necessary for the research or statistic concerned
 - c. it proves impossible to obtain explicit consent
 - d. the execution does not violate the privacy of the person concerned.

Article 9. Communication of personal data to other parties

1. Only if this is necessary for the execution of the above mentioned purposes, data will be provided to other parties. If Mohs Clinics has processor responsibility, processing agreements have been concluded with these parties to guarantee the protection of the personal data of patients and employees.
2. Mohs Clinics does not provide personal data to other parties, unless Mohs Clinics is legally obliged to do so (e.g. requesting personal data in the context of a police investigation).
3. No personal data will be provided to other parties outside the EU.

Article 10. Representation

1. If the person concerned (in this case the patient) is younger than 16 years of age, the parents/guardian will act in his/her place.
2. If the patient is 16 years of age or older and cannot be considered capable of a reasonable valuation of his interests, he shall act as his/her representative:
 - a. the trustee or mentor if the person concerned is under guardianship or has been appointed as a mentor on his/her behalf
 - b. a personal (written) representative, if any
 - c. any spouse or other life companion
 - d. a child, brother or sister, unless the person does not wish to do so
3. A person under the age of 18 may at any time appoint another person in writing to represent him in his place.

4. The consent may be withdrawn at any time by the data subject or his representative.
5. If a representative acts as a representative, the Foundation shall fulfil its obligations arising from the law and these regulations, unless such fulfilment is incompatible with the care of a good responsible party.

Article 11. Right of access and copy of recorded personal data

1. The data subject shall have the right to have access to the data relating to him.
2. The requested inspection will be provided within 4 weeks at the latest.
3. Important interests of others than the applicant, including the Board of the Mohs Clinics Foundation, may be a possible restriction for inspection.
4. A fee may be charged for the provision of a copy, up to a maximum of € 10 for the first 100 copies. However, the first copy shall be provided free of charge.

Article 12. Right to supplement, rectify or delete recorded personal data

1. On request, the recorded data shall be supplemented by a statement on the data provided by the data subject.
2. The data subject may request that the data be corrected if they are factually inaccurate, incomplete or appear in the processing in breach of a legal provision.
3. The data subject may request the deletion of data relating to him/her. This can have consequences for the continuation of the treatment agreement, because lack of medical information hinders a good quality diagnosis and good quality treatment.
4. The manager or treating specialist (if it concerns patient data or personal data) will provide a written message to the applicant, within 4 weeks after receipt of the written request for correction or removal, stating whether, and to what extent, the request is complied with. A refusal shall state the reasons on which it is based.
5. The manager or treating specialist shall ensure that a decision to correct, supplement, delete or destroy the data is implemented within 3 months of the request, unless it is plausible that the retention is of considerable importance to a party other than the person concerned.

Article 13. Right to data portability

This right, also known as the right to data transferability, means that patients or employees have the right to receive their own personal data that an organization processes from them. The parties involved can then save these data themselves for personal (re)use or pass it on to another organization. Mohs Clinics will not obstruct those involved in this and will ensure that they can easily obtain and pass on their data.

Article 14. Retention of data

1. With due observance of the legal provisions, the Board of Mohs Clinics Foundation determines how long the recorded personal data will be kept. These retention periods are:
 - a. for medical and care data: in principle 15 years, counting from the time they were manufactured, or as much longer as is reasonably necessary for good care by the care provider or the care of a good responsible party. The moment at which the document was made in Mohs Clinics is based on the last consultation of the patient.
 - b. for patients, data of a non-medical nature: no longer than necessary for the purposes for which they are processed, unless rendered anonymous, if they are kept for historical, statistical or scientific purposes.
 - c. for personnel data after termination of employment contract as long as required by law.
 - d. for applicant data: letter and CV will be destroyed four weeks after completion of the application procedure.
2. If the retention period of the data has expired, the (medical) personal data concerned will be deleted within 3 months.

3. Removal will not take place if it is plausible that the retention is of considerable importance to a person other than the person concerned, as well as retention on the basis of a statutory regulation is required or if there is agreement between the person concerned and Mohs Clinics Foundation.

Article 15. Complaints

If the data subject considers that the provisions of these rules are not being observed or has any other reason to complain, he or she may contact the Data Protection Officer (see data above). If it is not possible to find a solution with the data protection officer, the Board of Mohs Clinics Foundation can be contacted. The data subject also has the right to lodge a complaint with the Personal Data Authority, the supervisory authority in the field of privacy.

Article 16. Amendments, entry into force and inspection of these regulations

1. Amendments to these regulations are adopted by the Board of the Mohs Clinics Foundation and made by the general director.
2. These regulations entered into force on 1 October 2008. For recent changes in view of AVG see date above.