

INFORMATION DOCUMENT AND
RECORD OF PROCESSING ACTIVITIES

Drafted on: 16 February 2006
Updated on: 1 April 2019

EU General Data Protection Regulation (679/2016)

1. Data controller	Aava Medical Centre Ltd
2. Person in charge of the data file and contact persons	<p>Aava Medical Centre Ltd: Jukka Toivonen, Medical Director Annankatu 32, FI-00100 Helsinki, Finland tel. +358 (0)10 380 3800 (firstname.lastname@aava.fi)</p> <p>Unit managers and service managers in each unit act as respective contact persons: (tel. +358 (0)10 380 3800 or firstname.lastname@aava.fi)</p> <p>Aava Medical Centre Aviapolis, Tuija Koskelo Aava Medical Centre Hyvinkään Pipetti, Päivi Airola Aava Medical Centre Itäkeskus, Jaana Kiema Aava Medical Centre Järvenpää, Saira Kautonen Aava Medical Centre Kamppi, Hannele Fahlur (Regional Manager) Aava Medical Centre Karaportti, Henna Tolvanen-Mahjneh Aava Medical Centre Kerava, Pirkko Vanhanen Aava Medical Centre Keravan Terveyspuisto, Pirkko Vanhanen Aava Medical Centre Oulu, Mira Näyhä Aava Medical Centre Pasila, Jaana Kiema Aava Medical Centre Tampere, Marianne Vuorenmaa Aava Medical Centre Tapiola, Kaija Nyberg Aava Medical Centre Tuusula, Saira Kautonen Aava Medical Centre Turku, Sanna Kurppa (Occupational Health Nurse in charge)</p>
3. Data protection officer	<p>Ida-Emilia Laasonen Annankatu 32, FI-00100 Helsinki, Finland tel. +358 (0)10 380 3800 dpo@aava.fi</p>
4. Name of the data file	Centralised patient register of Aava Medical Centre Ltd and their self-employed partners.
5. Purpose of the processing of personal data / purpose of the data file	<p>The principal purpose of the data file is to plan, implement and monitor the examination and treatment of patients'/customers' health, illnesses and injuries and to process any related data.</p> <p>The register is also used for invoicing and collection purposes. Furthermore, the register is used for planning, developing, compiling statistics and following up of the data controller's own operations as well as for tasks related to the implementation of the rights and obligations of the data controller.</p> <p>Allowing the person's information to be stored in the patient register is a prerequisite for forming a treatment relationship with Aava Medical Centre. The processing of personal data is based on Aava Medical Centre's legal obligations to process patient data, a legitimate interest</p>

	<p>based on the patient relationship or the patient's consent or another relevant connection.</p> <p>The patient register ensures the monitoring of health care professionals and compliance with rules and regulations on private healthcare.</p> <p>Legislation governing the maintenance of the register: Act on the Medical Use of Human Organs and Tissues (101/2001) Act on the Status and Rights of Patients (785/1992) Act on the Electronic Processing of Client Data in Social and Health Care (159/2007) Act on Health Care Professionals (559/1994) Act on National Person Data Files in Health Care (556/1989) Act on Private Health Care Services (152/1990) Archives Act (831/1994) Decree of the Ministry of Social Affairs and Health on Health Records (298/2009) Decree on National Person Data Files in Health Care (774/1989) Decree on Private Health Care Services (744/1990) Employment Accidents Insurance Act (608/1948) Health Insurance Act (1224/2004) Motor Liability Insurance Act (279/1956) National Pensions Act (347/1956) The Data Protection Act (1050/2018) The EU general data protection regulation (679/2016)</p>
6. Content of the data file	<p>Basic information in the patient register:</p> <ul style="list-style-type: none"> • name • personal identity code • contact information (such as address, telephone, email address) • the guardian of an underage patient / a family member or another person close to the patient and their contact information and, if necessary, their personal identity code <p>Patient's consent to the processing and disclosure of data.</p> <p>Statutory patient records, including details of examinations and treatment provided</p> <ul style="list-style-type: none"> • health, illnesses and injuries; planning, implementing and monitoring examinations and treatment; any related information • vaccinations • laboratory and radiology examination data • results of examinations performed in the central laboratory • medical statements • any necessary data requested from other units • referrals to other units • data saved by psychologists, physiotherapists etc. • any other relevant information. <p>Name and title of the person who made the entry and date of entry.</p>
7. Regular sources of data	<p>The personal data stored in the patient register has been provided by the patient themselves or by the guardian of an underage patient. The correctness of personal data and contact details is verified at each appointment.</p> <p>Data, reports and statements related to examinations and treatment.</p>

	<p>Consultation results</p> <p>Documents obtained from other treatment or rehabilitation units with the permission of the patient/customer.</p> <p>Information provided via the online service.</p>
<p>8. Regular disclosure of data</p>	<p>Patient information is confidential, and those processing it are bound by an obligation of secrecy.</p> <p>Patient information may be disclosed primarily based on the patient's written consent. If the patient is not capable of assessing the significance of the consent, information may be given by his/her legal representative's written consent.</p> <p>In the case of further treatment, information necessary for the arranging of examination and treatment of the patient may be given to another health care unit or health care professional, and a summary of the treatment provided may be given to the health care unit or the health care professional that referred the patient for treatment and to a physician possibly appointed to be responsible for the care of the patient in accordance with the patient's orally-given consent or consent that is otherwise obvious from the context.</p> <p>Information necessary for arranging and providing the examination and care of a patient may be given to another Finnish or foreign health care unit or health care professional, if the patient, owing to mental health disturbance, mental handicap or for comparable reason is not capable of assessing the significance of the consent and he/she has no legal representative, or if the patient cannot give the consent because of unconsciousness or for comparable reason.</p> <p>Information about the identity and state of health of a patient may be given to a family member of the patient or to other person close to the patient, if the patient is receiving treatment because of unconsciousness or for other comparable reason, unless there is reason to believe that the patient would forbid this.</p> <p>Information in the patient register (including patient documents) is disclosed to authorities, such as the Parliamentary Ombudsman, The National Supervisory Authority for Welfare and Health, Regional State Administrative Agencies as well as insurance institutions, based on the special provisions set forth in the legislation. The aforementioned organizations process the confidential data disclosed to them in order to carry out their statutory duties and only for the purposes specified by law.</p> <p>In order to review the validity of a driving licence, the licence to carry firearms or other similar licence, the police have the right to obtain, upon a justified request, data related to a licence holder's health, substance use or violent behaviour regardless of any secrecy obligation, if there is a reason to suspect that the licence holder no longer meets the conditions of the licence.</p> <p>In addition, information in the patient register may be disclosed, regardless of any secrecy obligation, to authorities maintaining national registers, such as the cancer and infectious disease registers maintained</p>

	<p>by the National Institute for Health and Welfare and the Adverse Reaction Register maintained by the Finnish Medicines Agency Fimea.</p> <p>Personal data is disclosed, when necessary, to credit management and invoicing service providers for reminder and collection purposes. The data is always disclosed according to the Data Protection legislation and within the limits laid down by it.</p> <p>The data is disclosed as paper print-outs of electronic patient documents and copies of manual documents.</p>
<p>9. Transfer of data outside the EU or the European Economic Area</p>	<p>The data in the data file will primarily not be disclosed outside the European Union or the European Economic Area. The personal data of the data subject may be transferred outside the EU or EEA only with the data subject's specific consent or in exceptional cases to protect the vital interests of the data subject.</p>
<p>10. Storage, filing and disposal</p>	<p>The storing of patient documents and other material related to the treatment of the patient is the responsibility of the health care unit or private health care professional whose operations have generated the data in question.</p> <p>Patient information is stored in accordance with the Decree of the Ministry of Social Affairs and Health on Patient Documents (298/2009). Patient documents such as the documents containing the patient's basic information and essential treatment information, documents containing a statement of the patient's wishes, summaries, entries related to the planning, implementation, monitoring and assessment of treatment and the documents formed from those entries as well as referral, treatment feedback and consultation documents are kept for 12 years after the death of the patient, or if there is no information about the patient's death, for 120 years after the birth of the patient.</p> <p>The occupational health care team's examination and calculation materials as well as data collection forms such as individual documents related to the maintenance of employees' work ability (work ability index forms, work-related stress questionnaires and work ability profiles): for 12 years after the creation of the document.</p> <p>Documents concerning persons who have been examined or treated for occupational diseases: for 20 years after the patient's death, or if there is no information about the patient's death, for 100 years after the patient's birth and for 10 years after the end of the treatment.</p> <p>Detailed information regarding the storage periods of different kinds of documents can be found in the appendix of the Decree of the Ministry of Social Affairs and Health on Patient Documents (298/2009).</p> <p>Patient information will be filed in the national filing service (eResepti and eArkisto) maintained by the Social Insurance Institution of Finland in accordance with the Act on the Electronic Processing of Client Data in Healthcare and Social Welfare (159/2007) and the Act on Electronic Prescriptions (61/2007).</p> <p>When patient records are disposed of, it shall be ensured that outsiders cannot access the data.</p>

<p>11. General description of technical and organisational security measures</p>	<p>The data controller has taken appropriate technical and organisational measures to protect the data.</p> <p>Patient data may only be accessed by healthcare professionals involved in the patient's treatment at a given time and their assistants. Data may only be accessed to the extent required by the tasks of the healthcare professional.</p> <p>Manual documentation shall be stored in lockable archives, and only the persons who have the right to access them on the basis of confidentiality rules may access the documentation.</p> <p>Electronically stored data is protected through electronic access rights. Software applications and workstations require personal user credentials. The user name or password must not be disclosed to anyone. Usage of data systems and the access to the data in them is monitored separately for each username.</p> <p>Training and instructions were provided to employees when the software was deployed. IT support and main users were trained more extensively. New employees are trained and receive instructions as part of their job orientation. All employees sign a non-disclosure agreement at the time of signing their employment contract.</p>
<p>12. Right of access</p>	<p>Regardless of secrecy provisions, patients/customers shall have the right of access to the data on them in a personal data file.</p> <p>The right of underage persons to obtain information on themselves is determined according to general provisions on the right to be heard. Underage persons who, in the view of their age and maturity, are capable of making decisions on their treatment, may exercise the right of access independently. If an underage person who is capable of making decisions on treatment forbids the disclosure of the data to a parent or guardian, the latter shall have no right of access to patient register data.</p> <p>The right of access may be denied only in exceptional cases. Valid reasons for denying the access include that providing the information would cause serious danger to the patient's health or treatment or to the rights of someone else.</p> <p>The request to access patient data shall be made when visiting a clinic in person or by submitting a document that carries the person's own signature or is otherwise reliably verified. The identity of the persons exercising their access right shall be verified. Forms for requesting the right to access the patient register are available at the receptions of Aava Medical Centres and on the website.</p> <p>Patients/customers have the right to access their own patient records and obtain their information in writing on request. The access shall be provided without unnecessary delay, and the data shall be provided in a legible form. If necessary, a healthcare professional may explain the data.</p>
<p>13. Rectifications and their implementation</p>	<p>Aava Medical Centre, on its own initiative or at the request of the patient, without undue delay rectify, erase or supplement any data contained in the patient register if it is erroneous, unnecessary, incomplete or obsolete as regards the purpose of the processing.</p>

	<p>The request for rectification of patient data shall be made when visiting a clinic in person or by submitting a document that carries the person's own signature or is otherwise reliably verified. The patient's identity is verified before the request is processed. Forms for requesting rectification of data are available at the receptions of Aava Medical Centres and on the website.</p> <p>A health care professional will, together with a Senior Physician, assess whether there is cause for the rectification, erasure or supplementation of data.</p> <p>If the request for rectification is justified, the patient will be notified of the rectification of data recorded in the patient documents. If there are no grounds for rectification, a certificate of refusal, explaining why the request was refused, shall be provided.</p>
<p>14. Right to erasure ("right to be forgotten")</p>	<p>The patient has, under certain conditions, the right to have their data erased, also known as the right to be forgotten. The patient has the right to withdraw consent for the processing of their data and, after that, the right to submit a written request for the erasure of their data to Aava Medical Centre, insofar as the data is not processed in order to fulfil a legal obligation.</p> <p>The withdrawal of consent for the processing of personal data and the request for the erasure of personal data shall be made when visiting a clinic in person or by submitting a document that carries the person's own signature or is otherwise reliably verified. The identity of the person submitting the request shall be verified.</p>
<p>15. Right to restrict processing</p>	<p>The patient has the right to request Aava Medical Centre to restrict the processing of their personal data in situations such as when the patient is waiting for the data controller's response to their request for the rectification or erasure of their data.</p> <p>The request shall be made when visiting a clinic in person or by submitting a document that carries the person's own signature or is otherwise reliably verified. The identity of the person submitting the request shall be verified.</p>
<p>16. Right to data portability</p>	<p>The patient has the right to receive their data from the controller in a machine-readable format and to transmit the data to another controller. However, this requires that the patient themselves has provided the data in question to Aava Medical Centre.</p> <p>The request shall be made when visiting a clinic in person or by submitting a document that carries the person's own signature or is otherwise reliably verified. The identity of the person submitting the request shall be verified.</p>
<p>17. Right to lodge a complaint with a supervisory authority</p>	<p>The patient has a right to lodge a complaint with a supervisory authority if he/she considers that the processing of the personal data related to him/her infringes the General Data Protection Regulation.</p>
<p>18. Register administration</p>	<p>This information document and record of processing activities has last been updated on 1 February 2019. The data controller keeps track of the changes in the legislation and instructions by the authorities concerning</p>

	data protection and develops the operations of the service. This requires the data controller to reserve the right to update this record.
--	---