

DATA MANAGEMENT INFORMATION

on *MEDICAL CARE* related data management

1. DETAILS OF DATA CONTROLLER

Name:	ClinTrial Audit Health Services and Pharmaceutical Retail Limited Liability Company
Seat:	4032 Debrecen, Poroszlai út 110.
e-mail address:	mail@clintrial-audit.hu
represented by:	CEO Beáta Lénárt dr. Várkonyiné

2. SCOPE, PURPOSE, LEGAL BASIS, AND STORAGE LENGTH OF PROCESSED PERSONAL DATA

The personal data listed below are voluntarily supplied by you (e.g. appointment booking); their recording may also constitute a fulfilment of legal obligations (e.g. documentation of medical care).

Scope of personal data	Purpose of data processing	Legal basis for data processing	Length of data storage
<p>in relation to your identification: Surname and given name, Name at birth, Year/month/day of birth, Resident address, mother's name, signature, etc.</p> <p>In relation to contacting you: Phone number, e-mail address, etc.*</p> <p>in relation to your care: Medical records</p>	<p>medical counseling, provision of medical services</p> <p>auxiliary data handling, e.g. keeping contacts, appointment booking</p>	<p>legal obligation</p> <p>or</p> <p>*your consent</p>	<p>as prescribed by law</p> <p>or</p> <p>*until withdrawal of consent, up to 5 years after completion of care</p>

3. SOURCE OF PROCESSED DATA

Data controller will handle no data other than those obtained from you or your legal/authorized representative, and will either not collect/obtain data from third parties as a general rule or notify you when doing so.

4. ACCESS TO DATA, DATA PROCESSING, RECIPIENTS AND DATA SECURITY MEASURES

Access to data

The personal data listed in section 2 may be accessed primarily by the Data Controller.

Data processing, recipients

The data controller uses a data processor for data management (e.g. to operate an IT device, network, service). Upon request, the Data Controller promptly provides information on data processors used at the time.

As a general rule, the Data Controller will not directly (i.e. by data transfer) disclose your personal data processed in accordance with the above to any third person or organization, unless this is required or permitted by law (e.g. within the health system network: Electronic Health Service Space, beyond the health system network: authorities etc.).

Data security measures

The data storage location for Data Controller's own computer system and other (paper-based) data is at its headquarters/site of operation. The Data Controller shall select and operate the data storage devices used in such a way that the authenticity and authentication of the managed data is ensured and that their being unchanged can be verified.

5. RIGHTS RELATED TO DATA MANAGEMENT

<p><i>Right of access</i></p>	<p>You <u>may request information from</u> the Data Controller through one of the contact details provided in section 1 as to whether the processing of your personal data is in progress, and if so, you are entitled to find out which of your personal data are being handled by the Data Controller, on what legal basis, for what data processing purpose, and for how long. You also have the right to know: to whom, when, under what legislation did the Data Controller provide access, and to which of your personal data; to whom they transferred your personal data; the source of your personal data; whether the Data Controller uses automated decision-making, and if so, the logic thereof, including profiling.</p>
<p><i>Right to rectification</i></p>	<p>You <u>may request</u> by writing to one of the contact details provided in section 1 that the <u>Data Controller modify any of your personal data</u>; the Data Controller shall comply with the request within a maximum of one month.</p>
<p><i>Right to deletion</i></p>	<p>You <u>may request the Data Controller</u> by writing to one of the contact details provided in section 1 to <u>delete your personal data</u> processed under your consent.</p>
<p><i>Right to restrict</i></p>	<p>You <u>may request</u> by writing to one of the contact details provided in section 1 that your <u>personal data be restricted by the Data Controller</u> (by clearly indicating the limited nature of the data processing and ensuring that it is treated separately from other data). This lasts for as long as the reason you specify makes it necessary for the data to be locked.</p>
<p><i>Right to data portability</i></p>	<p>Concerning the data you voluntarily provided in section 2, you <u>may request</u> by writing to one of the contact details in section 1 to <u>receive</u> your personal data available to the Data Controller in a structured, widely used, <u>machine-readable format</u>; furthermore, you have the right for these data to be <u>transferred</u> by the Data Controller to another controller without hindrance.</p>

6. LEGAL REMEDY OPTIONS RELATED TO DATA MANAGEMENT

<p><i>Contacting the Data Controller</i></p>	<p>Your options include <u>contacting</u> the <u>Data Controller</u> directly with your questions, objections or complaints related to the above data management by the Data Controller.</p>
<p><i>Initiation of a legal court procedure</i></p>	<p>If you find that the management of your personal data is unlawful, you can <u>initiate a civil lawsuit</u> against the Data Controller in court.</p>
<p><i>Initiation of a supervisory authority procedure</i></p>	<p>If you notice any actual or potential unlawfulness in the management of your personal data during their handling as above, you <u>can contact</u> the National <u>Authority</u> for Data Protection and Freedom of Information, where you can <u>initiate an investigation</u> by submitting a report (contact details: website: http://naih.hu; address: 1125 Budapest, Szilágyi Erzsébet fasor 22/C; e-mail: ugyfelszolgalat@naih.hu).</p>

stamp
ClinTrial Audit LLC.