Appendix 1

Instructions for Data Processing

This appendix provides an overview of the personal data that the Controller may process within the framework of the Principal Agreement, and that may be assigned to the Processor. The appendix also contains information about, for example, the purpose, processing activities, locations for processing and data security linked to the Processor's processing of personal data.

Purpose

To fulfil the Processor's obligations under the terms of the Principal Agreement.

General remarks about personal data in the Processor's system

The Processor holds the general rights to the systems that the Processor provides to the Controller, with any deviations arising in the Principal Agreement.

The Processor's point of departure is that all data entered into the system by the Controller, or anyone acting on behalf of the Controller, for example regarding users and patients, is the property of the Controller. That the Controller registers data in any of the Processor's systems does not therefore automatically infer that the Processor is the processor of the data, which they only become in cases where they in some way process the personal data in question. The Processor carries out processing on behalf of customers in accordance with each Principal Agreement, primarily where the Processor provides operation of the system for the Controller, communicates personal data from and to other systems or when carrying out consultancy assignments (e.g. data migration, registration of data on behalf of the Controller, correction as instructed by the Controller).

The Controller is always responsible for ensuring that the collection and registration of data, information to data subjects, deletion procedures and other legal requirements regarding the collection and handling of personal data are implemented in accordance with applicable legislation and regulations. The Processor is solely responsible for ensuring that the processing carried out by the Processor under the terms of the Principal Agreement is carried out in accordance with this Agreement.

Categories of data subject

All categories of data subject that the Controller may register/assign, primarily consisting of;

patients/students/employees/users/others that use or have the right to use the customer's services, care recipients' relatives and other contacts, employees (users) of the customer, consultants/employees of subcontractors, healthcare staff or others who are not employed by the customer but that have some other connection to the patient (those sending/receiving referrals from a different healthcare unit/laboratory, other school staff, staff at other public authorities or the like).

Data categories

For employees/consultants of the Controller (please note that not all data is applicable to all employees/consultants);

name and contact information, personal identity number, professional role, expertise, codes linked to the person (e.g. HAS ID, employee number, prescription code, etc.), authorities, log-in information (e.g. time stamps, access) and similar information.

For care recipients (please note that not all data is applicable to all care recipients);

name and contact information, personal identity number, other types of personal codes and IDs, gender, medical and health data, payment information, appointments, country of birth, native language, family situation, family relationships, relatives, consent data, school/class and company affiliation. Please note that data may even include notes such as free text in journals and other areas of the system (all types of personal information may be included in these free text fields and it is not unusual to find sensitive personal data other than medical and health data).

Other registered individuals (see under heading "Categories of data subject" above for the types of person this may refer to, please note that not all data is applicable to all care recipients);

name and contact information, personal identity number, professional role, workplace, codes linked to the person (e.g. HAS ID, employee number, prescription code, laboratory code) relation to/events related to/contacts/discussions regarding/minutes/memos including/concerning care recipients and similar data. Please note that data may even include notes such as free text in journals and other areas of the system (all types of personal information may be included in these free text fields and it is not unusual to find sensitive personal data other than medical and health data).

Processing activities

Below is a list of the activities that may be carried out by the Processor within the framework of data processing under the terms of the Principal Agreement.

Storage, processing or changes, collection, registration, structuring, production, reading, use, adjustment or aggregation, transfer, restriction, erasure or destruction, correction or troubleshooting on behalf of the Controller based on what has been agreed between the Controller and Processor in the Principal Agreement, as well as in accordance with instructions issued in specific cases to the Processor's support, consultation, development or operations departments or other employees of the Processor.

Location where personal data will be processed

For all customers;

Processing may be carried out by employees of the Processor at the company's Swedish offices in Uppsala, Stockholm and Gothenburg, at the premises of the Controller when the Processor's personnel provide on-site support or installation, or on site by or at the premises of sub-processors as listed in Appendix 2.

Physical storage for customers using the Processor's hosting service in Sweden;

Data centre in the Gothenburg area, Sweden.

Physical storage for customers using the Processor's hosting service in Germany;

Data centre in Frankfurt, Germany.

Data security

The protection of customers' personal data assets is a matter of priority for the Processor. The basic principles underlying the Processor's data security are; availability, accuracy, confidentiality and traceability.

Flaws in data security may cause disruption to the vital public services provided by customers and entail a risk to the rights and freedoms of data subjects. The Processor shall therefore comply with the following guidelines in order to ensure that the above-named principles are adhered to with regard to all personal data processing:

- Identify, risk-manage and assign responsibility for personal data assets and take relevant, balanced security measures to protect this data.
- Manage data availability in accordance with applicable legislation, policies and guidelines, and the customer's instructions.
- Educate and inform employees regarding data security in order to achieve and maintain a good level of training and ensure that appropriate data security measures are applied.
- Design, implement and maintain procedures and tools for monitoring that ensure data security.
- Design, implement and maintain routines and tools for managing personal data breaches.
- Control employees' access to data; i.e. the right information at the right time and right place to an authorised user.