PROCESSING OF PERSONAL DATA

1 Introduction

2This Appendix concerning the processing of personal data (”Appendix”) is an inseparable part of the Agreement between Nightingale Health Ltd (”Nightingale”) and the Customer regarding NMR-based Quantitative Metabolomics Platform Analyses.

Any term not otherwise defined herein shall have the meaning specified in the General Terms and Conditions.

As a part of the Service, Nightingale shall, on behalf of the Customer, process Personal Data. Duration of processing the Personal Data is defined in the Agreement.

2 Data Protection and Processing Personal Data

2.1 Type of Personal Data and Data Subjects

Personal Data means any information relating to an identified or identifiable natural person (“Data Subject”). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

When performing the Service, Nightingale may process the following types of Personal Data:

i. Samples;
ii. Sample identification number;
iii. Clinical Data related to data analysis Service; and
iv. Results of the Service such as original NMR-data, spectral data and quantified metabolomic data derived from the Samples.

Any Personal Data provided to Nightingale shall be in pseudonymized format, i.e. the personal data cannot be attributed to a specific Data Subject without the use of additional information. Such additional information shall not be provided to Nightingale.

The Data Subjects for the processing under the Agreement are the sample donors of the Samples from which the Service Deliverables are generated.

2.2 General Obligations of the Parties

The Customer is the Controller of the Personal Data and Nightingale is the Processor of the same. As the Controller, the Customer is responsible for ensuring that it has the necessary rights and has acquired the necessary consent to process the Personal Data.

The Customer is responsible for drafting a record, keeping it accessible and informing the Data Subjects according to applicable data protection legislation.

Nightingale has the right to process Personal Data only in accordance with the Agreement, this Appendix and the written guidance of the Customer.

The personnel of Nightingale and its subcontractors shall commit to maintain the confidentiality of the Personal Data.

If the processing of the Personal Data by Nightingale or its subcontractor takes place in a country outside of the EU/EEA, Nightingale shall endeavor, in accordance with the applicable legislation, to manage the special requirements (i.e. the adequate level of protection) of such Personal Data transfers.

Nightingale shall forward all requests to inspect, rectify, erase, ban the processing of data or other requests received from the Data Subjects, to the Customer. The Customer has the responsibility to respond to such requests. At Customer’s request, Nightingale supports Customer in carrying out the statutory requests of the Data Subjects, insofar as possible taking into account the nature of the processing.

Nightingale shall direct all inquiries of the data protection authorities related to Personal Data to the Customer. Nightingale shall notify the Customer of any measures taken by data protection authorities in connection with handling of Personal Data.

2.3 Sub-processors

Nightingale may engage sub-processors in processing the Personal Data. Nightingale will make available to Customer a list of current sub-processors at https://nightingalehealth.com/subprocessors updated from time to time.

The Customer shall notify Nightingale of any reasonable grounds to oppose the use of a certain sub-processor promptly, but no later than fourteen (14) days after receiving a notice from Nightingale regarding respective sub-processor.

Nightingale shall sign written contracts with its sub-processors and shall ensure that its sub-processors will adhere to similar technical and organizational security measures as described in this Appendix. Nightingale shall regularly supervise the actions of its sub-processors and shall be liable for the acts of its subcontractors as if they were Nightingale’s own.

2.4 Audit Rght

If requested, Nightingale makes available to the Customer information necessary to demonstrate compliance with its data protection obligations under the Agreement in the following manner. Based on thirty (30) working days’ notice provided by the Customer in writing, authorized third-party auditor which is accepted by both Parties may inspect Nightingale’s compliance with this Appendix.

A third-party auditor shall be obliged in writing to maintain confidentiality in all matters related to the audit. The audit shall not unreasonably interfere with Nightingale's day-to-day business operations. The Customer shall carry its costs caused by the audits.

If an audit shows any deficiencies or non-compliance of the data protection clauses of this Appendix by Nightingale, Nightingale shall as a sole and exclusive remedy inspect and rectify its operating models in a manner determined by Nightingale and report taken actions to the Customer.

2.5 Data Retention or Erasure

After the delivery of the Service Deliverables to the Customer, Nightingale is entitled to retain the Analysed Sample Material, Sample identification numbers, original NMR-data, spectral data and quantified metabolomic data derived from the Samples for the purposes of quality control of the Service and for the purposes of providing additional service which may be agreed separately between Nightingale and the Customer. Nightingale has no obligation to store the Analysed Sample Material or any of the above-mentioned Personal Data, and Nightingale may destroy the Analysed Sample Material or any of the above-mentioned Personal Data after performing the Service.

The Customer may with a separate written notice request Nightingale to destroy the Sample identification numbers relating to the Customer’s Samples. After destroying the Sample identification numbers, the results of the Service can no longer be attributed to a specific individual even with the help of additional information processed by the Customer, and the use of such anonymized results for the above mentioned purposes is no longer possible.

3 Technical and Organizational Security Measures

Nightingales internal organization is structured in a way that it meets the requirements under this Appendix and the data protection laws applicable to its operations.

Nightingale has implemented the following appropriate technical and organizational measures to secure the Personal Data when providing the Service to the Customer.

The Customer accepts the measures to secure the Personal Data described in this Appendix as appropriate and sufficient technical and organizational measures for securing the Personal Data.

3.1 Personnel Security

Employees are selected based on their level of education, skills, experience, competence and person's suitability to the position. Employee's experience and education are verified by interviewing the employee and from the employee's CV. All Nightingale's employees have a job description which defines the responsibilities and qualifications for each job position. The job descriptions are part of Nightingale's quality system.

Access rights to information management systems and to physical locations are granted based on the role described in the employees' job description. Access rights are monitored regularly and updated according to changes in roles and/or employment status.

In order to ensure that the data processing is in accordance with applicable data protection legislation and Customer's instructions, all employees are trained on the proper use of software modules and the importance of data security. The training covers necessary security and safety matters, such as ensuring the confidentiality of Personal Data and preventing exposure of Personal Data to non-authorized persons.

To verify the comprehensive training of all employees, the training plans and completed trainings are documented and archived.

Nightingale monitors employees' compliance with data protection regulation and Customer's instructions on a regular basis. Effectiveness and actualization of trainings is assessed during the training sessions and by monitoring the work done by the employees.

Nightingale shall notify its Customers of any breach or non-compliance by Nightingale of any applicable data protection law as soon as reasonably possible after becoming aware of such breach or non-compliance and document responsive actions taken in connection with any incident involving a breach of security. If deemed necessary, Nightingale shall make changes in its business practices relating to protection of Personal Data to prevent similar breaches or non-compliances in the future.

3.2 Physical Security

Nightingale utilizes the following physical workspaces for its Service:

- Nightingale Data centre, where physical servers operated by Nightingale are located;
- Laboratories, where Samples are prepared and measured; and
- Office workspace, where authorized users may operate the Service.

The data centre, laboratories and office work spaces are protected with electronic locks. Access to different physical locations is authorized only to employees who need to have access based on their role and tasks in connection to providing the Service.

Service providers providing ancillary services are carefully selected and reasonable steps are taken to ensure that such service providers are capable of maintaining appropriate security measures consistent with this Appendix. Third parties are allowed to visit physical workspaces only under surveillance and visitor details are logged.

Received Samples and possible Personal Data in paper format are stored only in the laboratory and can be accessed only by Laboratory Operators. Personal Data on paper format is archived into a locked area accessible only by authorized persons.

3.3 Data Communication Security

Site-to-site VPN secures the communication between the subnets using a strongly encrypted tunnel. All Nightingale subnets are secured with firewalls having content filtering, malware protection and intrusion prevention. All network infrastructure including security rules, subnet configuration and access rules are managed centrally using management tools authorized only to System Administrators and requiring two-factor authentication.

Software that processes information related to sample handling and measurement can only be accessed from laboratories or with L2TP secured VPN connection from outside laboratories.

Personal workstations in the office workspace use the wireless network, which is secured using WPA2 protocol.

No third party has access to Nightingale networks or devices.

3.4 IT Security

Nightingale's employees utilize personal workstations, which are standardized according to Nightingale's security work instructions. All personal workstations have built-in security protection including firewall protection, and their storages are encrypted. Employees are instructed to lock their personal workstations when leaving the workstation. Only software defined in the security work instructions can be installed into personal workstations. If a personal workstation is sent to maintenance, all information is removed and the access to removed information is prevented through disk encryption.

Servers in Nightingale's on-premises data centre are located in a dedicated machine room, physically accessible only by System Administrators. The management tools for servers in the data centre can be accessed only using L2TP secured VPN connection, which is authorized only for System Administrators. Non-personal administrative accounts (user ids and passwords) are stored in a secure storage accessible only by System Administrators. Administration operations are recorded into a system change log.

Nightingale may also use a third party computing provider (Cloud service) for running the Service. In this case, Nightingale ensures, that the selected third party Cloud service provider guarantees to

- be in compliance with ISO27001 standard;
- be in compliance with applicable data protection regulation; and
- adhere to the CISPE Code of conduct allowing the choice to store and process Nightingale's data entirely within the European Economic Area.

3.5 Information Security

Personal Data can be processed for the purpose of providing the Service as agreed between Nightingale and the Customer. Any access rights for other purposes, such as Nightingale's research and development activities, are agreed between Nightingale and the Customer in writing.

Access to the Personal Data is restricted to only those who need such information to perform their job duties. Software systems secure access by using a personal user id and password.

Laboratory Operators can access only Personal Data allocated to a specific laboratory belonging to the respective area of responsibility. Laboratory Operator's actions for preparing and measuring samples and Data Analyst's actions for releasing the results are logged. Log data can be used to identify the persons handling Personal Data as well as actions performed and time for such actions.

Access to the Results of the Service provided to the Customer is protected by using a user id and password which are delivered in a secure way to determined Customer contact person.

3.6 Availability Control

Nightingale has implemented appropriate fault tolerance by ensuring that a failure in a single device does not cause service downtime or data loss. The data is backed up daily into a geographically separated location.

Nightingale has a documented process to investigate any problems in the Service, inform required parties, correct the problem and return the Service into normal use as soon as reasonably possible.

4 Revisions of this Appendix

Nightingale shall be obligated to inform Customer in writing of all changes that may affect its ability or prospects to abide by this Appendix and the written guidance of the Customer.

Any additions or changes to this Appendix shall be agreed in writing.