USE AND DISCLOSURE OF PERSONAL INFORMATION

1 Introduction

This Appendix concerning the use and disclosure of Personal Information ("Appendix") is an inseparable part of the Agreement between Nightingale Health United States, Inc. ("Nightingale") and the Customer regarding NMR-based Quantitative Metabolomics Platform Analyses for Research Use.

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, use and disclose Personal Information for the period defined in the Agreement.

2 Use and Disclosure of Personal Information

2.1 Type of Personal Information and Individuals

Personal Information means any information relating to a natural person ("Individual") that either identifies that Individual directly or creates a reasonable basis to believe the information can be used to identify the Individual. Personal Information is no longer Personal Information when it has been de-identified in accordance with applicable laws and regulations such that the Individual is no longer identified or identifiable using reasonable efforts, resources, and technology.

When performing the Service, Nightingale may use and disclose the following types of Personal Information:

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

Any Personal Information provided to Nightingale shall be limited to the minimum necessary for its intended purpose and, where appropriate, shall be in the form of a limited data set in accordance with 45 C.F.R. § 164.514(e) or de-identified by Customer in accordance with applicable laws and regulations. Should Customer de-identify the Personal Information, Customer may assign a code or other means of record identification to allow re-identification by Customer, provided that such code or other means of record identification shall not be derived from or related to the Personal Information and shall not be capable of being translated to identify the individual. Such code or other means of record identification shall not be provided to Nightingale.

The Individuals for the use and disclosure of Personal Information 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 responsible for ensuring that it has the necessary rights and has acquired the necessary consent for Nightingale to use and disclose the Personal Information to perform the Service.

The Customer is responsible for maintaining accountings of disclosures and other logs and records according to applicable privacy and data protection laws and regulations.

Nightingale has the right to use and disclose Personal Information 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 Information.

When Nightingale transfers Personal Information outside of the EU/EEA, it will comply with laws applicable to such transfers.

Nightingale shall forward all requests to inspect, amend, erase, restrict uses or disclosures, or other requests received from the Individuals, 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 Individuals as practicable based on the request.

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

2.3 Subcontractors

Nightingale may engage subcontractors in performing the Service who may handle Personal Information. Nightingale will make available to Customer a list of current subcontractors 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 subcontractor promptly, but no later than fourteen (14) days after receiving a notice from Nightingale regarding respective subcontractor.

Nightingale shall sign written contracts with its subcontractors and shall subject its subcontractors to similar requirements for technical and organizational security measures as described in this Appendix.

2.4 Audit Right

If requested, Nightingale makes available to the Customer information necessary to demonstrate compliance with its privacy and data protection obligations under the Agreement in the following manner. Based on thirty (30) business 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 with the provisions 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 Deletion

After the delivery of the Service Deliverables to the Customer, Nightingale is entitled to retain the Analyzed 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 Analyzed Sample Material or any of the above-mentioned Personal Information, and Nightingale may destroy the Analyzed Sample Material or any of the above-mentioned Personal Information 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 de-identified results for the above mentioned purposes is no longer possible.

3 Technical and Organizational Security Measures

Nightingale's 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 Information when providing the Service to the Customer.

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

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.

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 Information and preventing exposure of Personal Information to unauthorized persons.

To verify the comprehensive training of all employees, 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 of their Personal Informationas soon as reasonably possible after becoming aware of such breach 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 Information to prevent similar breaches in the future.

3.2 Physical Security

Nightingale utilizes the following physical workspaces for its Service:

- Nightingale Data center, 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 center, 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 Information in paper format are stored only in the laboratory and can be accessed only by Laboratory Operators. Personal Information 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 is authorized to access 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 center 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, the selected third party Cloud service provider agrees to

- be in compliance with ISO27001 standard; and
- be in compliance with applicable data protection regulation.

3.5 Information Security

Personal Information can be used and disclosed 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 Information 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 Information 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 Information 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 to minimize the likelihood that a failure in a single device causes 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.