QuantHealth Privacy Policy

1. Introduction

Quant Health Ltd. is committed to ensuring the privacy and protection of personal data in accordance with relevant privacy legislation, including the General Data Protection Regulation (GDPR) and other applicable data protection laws. This Internal Privacy Policy provides guidelines, instructions, and internal policies to ensure that Quant Health Ltd. employees, contractors, and collaborators adhere to the highest standards of data privacy and security.

The company specializes in developing advanced artificial intelligence models designed to predict and optimize clinical trial outcomes, ultimately enhancing the effectiveness of trial protocols. Importantly, these models do not require the use of personal information, as the experimental protocols and criteria are focused on meeting specific needs without necessitating the processing of identifiable personal data.

However, while developing the models and engaging in collaborations, the company may occasionally encounter and process information that could be related to personal information or be considered personal information under certain regulations. In this context, it is worth noting that the company predominantly utilizes de-identified information in accordance with HIPAA provisions, which has been validated by a reputable provider in the field for research purposes.

Nevertheless, within the scope of the company's operations—including communication with clients, marketing activities, and employee recruitment—some information may be considered "personal information." As a result, the company has implemented a comprehensive set of procedures aimed at protecting, securing, and maintaining the privacy of this information. This policy serves as a guiding framework that outlines the principles and practices related to privacy and data protection within the company.

2. Scope

This policy applies to all employees, contractors, and collaborators of the company who handle personal data in their work. Personal data includes any information that relates to an identified or identifiable individual, such as names, addresses, email addresses, phone numbers, and health-related data, to the extent exist, accessed, or processed by the company.

3. Privacy Principles

The company adheres to the following privacy principles in its handling of personal data:

- Lawfulness, fairness, and transparency: Personal data must be processed lawfully, fairly, and transparently.
- Purpose limitation: Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
- Data minimization: Personal data must be adequate, relevant, and limited to what is necessary for the purposes for which they are processed.

- Accuracy: Personal data must be accurate and, where necessary, kept up to date.
- Storage limitation: Personal data must be kept in a form that permits identification of data subjects for no longer than necessary for the purposes for which the data is processed.
- Integrity and confidentiality: Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and accidental loss, destruction, or damage.

Those principles are demonstrated within the company's set of policies and procedures, as well as in the company's analysis, mapping, and mitigation when processing data which was derived from personal data.

4. Responsibilities

All employees, freelancer employees, and collaborators of the company are responsible for:

- Complying with this Internal Privacy Policy and related procedures.
- Reporting any suspected data breaches or privacy concerns to the Data Protection Officer (DPO).
- Participating in privacy training and awareness programs provided by the company.

5. Protection Officer (DPO)

Quant Health Ltd. has designated a Data Protection Officer (DPO) to oversee and ensure compliance with this Internal Privacy Policy and relevant privacy legislation. The DPO is responsible for:

- Informing and advising the company about its obligations under applicable privacy regulation;
- identification of processing activities of personal data and providing the company with guidance and instructions to ensure its proper and secured manner;
- monitoring compliance with the applicable privacy regulation, company's data protection policies, awareness-raising, training, and audits;
- cooperating with any data supervisory authorities on behalf of the company;
- acting as a contact point for data subjects and processing their inquiries related to the Company's data processing activities;
- ensuring the performance of initial and periodic information privacy risk assessments and conducting ongoing compliance monitoring activities;
- providing the proper management of relevant data incidents, including the filing of required reports in accordance with applicable privacy regulation;
- Maintains, directly or through the company's legal advisors, current knowledge of applicable international, federal, and state privacy laws and accreditation standards and monitors advancements in information privacy technologies to ensure the Company's adaptation and compliance.

6. Data Collection and Processing

The company shall ensure that anytime personal data is being collected or processed:

- Personal data is collected and processed only for legitimate purposes. Where such data is collected for product development and is health-related, such data will always be de-identified

before used for developing such AI algorithms, unless an explicit lawful consent was obtained as instructed by company's legal advisors.

- Data subjects are informed about the purposes of data collection, the legal basis for processing, their rights, and any recipients or categories of recipients of the personal data.
- Consent is obtained from data subjects when required by law.
- Privacy impact assessments are conducted when necessary to identify and mitigate privacy risks associated with new projects, technologies, or processes.

7. Data Storage and Security

The company maintains appropriate technical and organizational measures to protect personal data (and any other sensitive data) against unauthorized or unlawful processing and accidental loss, destruction, or damage. These measures further detailed in company's security procedures and include:

- Secure storage and transmission of personal data.
- Regular security audits and updates to software and hardware.
- Restricted access to personal data on a need-to-know basis.
- Security training and awareness programs for employees, contractors, and collaborators.

The company has adopted a Code of Conduct for the employees, providing simple and straightforward instructions regarding the expected secured conduct. Each new employee is being provided with the Code of Conduct and proper training upon hiring.

8. Data Retention and Destruction

The company retains personal data only for the period necessary to fulfill the purposes for which it was collected or as required by law. Personal data that is no longer needed is securely destroyed or anonymized in accordance with established data retention and destruction procedures. Retention periods shall be defined clearly in the company's mapping documentation.

9. Data Subject Rights

The company respects the rights of data subjects under applicable privacy laws, including the right to access, rectify, erase, restrict processing, object to processing, and data portability. Data subjects may exercise their rights by contacting the DPO. The company shall address data subject inquiries in accordance with its designated procedures, setting a clear easy-to-follow organizational flow ensuring that any such inquiry will be dealt with efficiently.

10. Data Breach Response and Notification

In the event of a personal data breach, Quant Health Ltd. has established procedures to:

- Investigate and contain the breach to prevent further unauthorized access, disclosure, or damage.
- Notify the DPO and CEO and nominate a designated team who will coordinate the response and determine whether the breach is likely to result in a risk to the rights and freedoms of data subjects.

- Notify affected data subjects and supervisory authorities when required by law, providing information about the nature of the breach, the steps taken to address it, and the measures taken to mitigate its potential adverse effects.
- Document the breach, including its facts, effects, and remedial actions taken.

11. Training and Awareness

Quant Health Ltd. provides privacy training and awareness programs for employees, contractors, and collaborators to ensure that they understand their responsibilities under this Internal Privacy Policy and relevant privacy legislation including the GDPR and HIPAA. Training includes information on the principles of data protection, data subjects' rights, the responsibilities of the employees, the procedures for handling personal data and reporting data breaches and general knowledge regarding data security and proper IT conduct in accordance with company's relevant policies and procedures.

12. Policy Review and Updates

This Internal Privacy Policy will be reviewed at least annually or whenever there are significant changes to privacy legislation or Quant Health Ltd.'s data processing activities. Updates will be communicated to all employees, relevant contractors, and collaborators, who are expected to adhere to the revised policy.

13. Compliance and Enforcement

Failure to comply with this Internal Privacy Policy may result in disciplinary action, up to and including termination of employment or contractual relationship. Any concerns about non-compliance should be reported to the DPO.

By implementing and enforcing this Internal Privacy Policy, Quant Health Ltd. demonstrates its commitment to maintaining the privacy and security of personal data in accordance with privacy legislation, including the GDPR, and upholding the trust of data subjects and partners.