RiAtlas quality policy is dedicated to all end users of our products. More specifically, this document is dedicated to patients potentially interested in our services and activities and other interested parties, including our staff, customers, clinical institutions, business partners, suppliers, patient and physician organizations, and the competent authorities.

Our quality policy is a declaration of intent concerning all aspects of our company life, emphasizing our focus on patients' safety and health in a fragile condition in their home daily lives.

Our dedication to customer satisfaction, through continuous research, enhances the collection of real-life, real-world data in a non-invasive manner.

Our dedication to maintaining the company system's efficacy with the aim to consolidate patient safety through technological innovation techniques.

Our aspirations of continuous improvement employing technological innovation via personalization and incremental training of our AI model.

The objective of the quality policy is to provide to the company personnel awareness on:

- Developing a product to improve patients' quality of life and data quality for their clinical path management.
- Ensuring that each product placed on the market complies with legal and regulatory requirements, including the Medical Devices Directive.

To ensure customer and end-user satisfaction, the Company will:

- Certify the quality of our products and services following international standards.
- Strive to define and test new versions of our systems regarding continuous control of our AI model's changes and improvements and our user interface.
- Ensure that patients in a fragile state after hospital discharge receive a state-of-the-art solution to support and improve their life at home while providing increased quality and quantity of data to their medical professionals.

To ensure patient safety and health, RiAtlas will:

- research innovative solutions to collect valuable data in real-time during the home recovery of fragile patients after hospital discharge, in compliance with European guidelines on respectful AI models.

To ensure compliance with Regulatory requirements, since Riatlas is dedicated to the design, manufacture, and distribution of high-quality and safe medical devices, its quality management system is certified in accordance with ISO 9001, ISO 13485, and ISO/IEC 27001, ensuring that all the processes systematically address product quality, regulatory compliance, and information security.

In full alignment with Article 10 of the MDR, Riatlas commits to:

- *Implementing and maintaining a comprehensive integrated Quality Management System that covers all aspects of product lifecycle management, including risk*

management, clinical evaluation, performance validation, and traceability (Article 10(9)(a)).

- *Ensuring that all devices placed on the market comply with the applicable General Safety and Performance Requirements as outlined in Annex I of the MDR and that conformity assessment procedures under Article 5 are rigorously applied (Article 10(9)(b) + Article 5(2) + Annex I).*
- *Assigning the responsibility for management and management of resources, including the selection and control of suppliers and subcontractors. (Article 10 (c) (d))*
- *In particular, as specified in Article 10(9) of the MDR, we ensure that our Quality Management System comprehensively addresses:*
    - *A systematic process for risk management, covering design, manufacturing, and post-market phases, to proactively minimize risks associated with device use (Article 10(9)(e)+ Annex I Chapter I, Section 3);*
    - *Clinical evaluation and validation procedures, ensuring that our devices consistently achieve their intended purpose and maintain an acceptable benefit-risk profile throughout their lifecycle (Article 10(9)(f) + Article 61 + Annex XIV);*
    - *The realization of the product, including planning, design, development, production, and service delivery (Article 10(9)(g);*
    - *Verification of the UDI assignments carried out in accordance with Article 27 ensuring the consistency and validity of the information provided (Article 10(9)(h));*
    - *Post-market surveillance systems, designed to actively and systematically collect, record, and analyze relevant data on the quality, performance, and safety of devices after they have been placed on the market. These systems allow us to identify any need for corrective or preventive actions, thereby maintaining a high standard of patient safety and product performance togheter with eporting of serious incidents and the implementation of safety corrective actions within the framework of vigilance activities (Article 10(9)(i)(k)(l) + Articles 83 + Annex III);*
    - *The management of communication with competent authorities, notified bodies, other economic operators, customers, and/or other relevant stakeholders (Article 10(9)(j));*
    - *Documented procedures shall be established to ensure the systematic monitoring and measurement of process and product performance, the thorough analysis of relevant data, and the implementation of actions aimed at enhancing product quality and continuous improvement Article 10(9)(m)).*

RiAtlas Quality Policy reflects its commitment to maintaining regulatory compliance, upholding the highest standards of product quality and patient safety, and protecting the confidentiality, integrity, and availability of sensitive information handled within our data flows.

In addition, RiAtlas adopts the following information security management policy:

“Declare its commitment to create and maintain an Information Security Management System, in which the risks are subject to controlled management to prevent and limit damage to the information circulating within the Company, with the aim of other than:

- Ensure the security of information within the organization’s processes.
- Guarantee the maximum security of customer information regarding confidentiality, availability, and integrity of the information itself, providing a service with high added value, thanks to customer data segregation.
- Give operational continuity to critical services even following serious incidents capable of compromising the Company’s survival.
- Protect the rights and interests of all those who interact with the Company (so-called stakeholders: customers, suppliers, employees, collaborators, third parties, etc.).
- Safeguard the interests of investors and partners.
- Guarantee an excellent level of service.

RiAtlas S.r.l. through its employees’ participation undertakes to ensure compliance with the legislative provisions on security, data protection and with any other agreement signed with the interested parties. RiAtlas S.r.l. pursues the continuous improvement of its Information Security Management System, identifying the following principles:

- Provide an essential support service to the Company’s Core Business through tools and means technologically in line with progress and keeping them in a perfect state of efficiency.
- Define the roles and responsibilities of the personnel involved in the management of Information Security.
- Manage application and organizational changes in accordance with the reference standards and in a structured manner.
- Choose the best risk management strategy according to the type of risk to which the Company is exposed and the possibilities of intervention by the Company itself. Each “High” level risk will be assigned an intervention manager who will be entrusted with implementing the countermeasures validated by the Management. All “low” and “medium” risks will be accepted.
- Adopt a structured process to manage information security incidents to contain their impacts, identify their causes, and encourage their removal. All subjects affected by the ISMS are required to report anomalous or suspicious circumstances regarding the information.
- Periodically and systematically identify the data’s threats, assess the exposure to risks, and take steps to implement suitable preventive actions.
- To train personnel to carry out activities to protect company assets in compliance with current legislation.
- Encourage the dissemination of culture and awareness of the security and protection of data and information, particularly the confidentiality, integrity, and availability of data and information, among its employees, collaborators, partners, and third parties regarding their roles and responsibilities in this area.

- To deal quickly, effectively, and scrupulously with emergencies or accidents that may occur in carrying out the activities, also collaborating with third parties or responsible bodies.
- Respect the laws and regulations in force in this context, and in any case, abide by standards identified with a sense of responsibility and awareness based on scientific principles and risk assessment.
- Carry out monitoring and review activities, starting with the most critical ones, updating the safety programs planned to achieve and ensure this policy."

RiAtlas undertakes, regarding the security of its cloud services, to implement the following additional principles:

- Consider basic information security requirements applicable to cloud service design and implementation (Service Availability, Incident Response, Service Elasticity, and Load Tolerance, Data Lifecycle Management, Technical Compliance and Vulnerability, Change Management, Data Isolation, Log Management, and Forensics);
- adopt measures to prevent risks from internal intrusions (authorized workers);
- implement multi-tenancy and ensure customer isolation of cloud services (including virtualization);
- ensure the security of access to the client's resources of the cloud service;
- implement access control procedures;
- provide timely communications to cloud service customers while managing change;
- apply virtualization security by limiting access to virtual machines, tightening system protection, applying change management and malware protection rules, periodically monitoring and verifying resources, etc.;
- guarantee access and protection of the data of the customers of the cloud service;
- manage the life cycle of cloud service customers' accounts;
- Communicate violations and provide guidelines on sharing information to aid investigations and forensic (investigative) activities.

RiAtlas undertakes, concerning the management of personal data of its cloud services, to implement the following additional principles:

- Compliance with current legislation in terms of personal data processing where RiAtlas acts as Data Processor on behalf of customers (Healthcare Facilities, etc.) who instead configure themselves as Data Controllers to process patient data managed by the cloud platforms object of the services. The application of Italian / European legislation is currently envisaged.
- Identification of the respective responsibilities regarding the data processing of their CLOUD services, provided in SaaS mode, both in the acceptance of the respective positions as Manager and in the internal appointments that also define the contact point that the customer can contact for any need about the processing of the data.

The Board of Directors of RiAtlas intends to:

- provide enough resources to the company system and ensure the continuous maintenance and update of infrastructure and personnel competence.
- Ensure that the Quality system is an integral part of company life.
- Promote the quality policy through measurable goals that are monitored over time.
- Define a good surveillance and vigilance system.
- Upgrade this policy as per requirements and as per state of the art.

The Chairman and Legal Representative