TECHNICAL SPECIFICATIONS
For the Open Tender
"Cloud-based software development, including a database, analytics, and other functionality"
(identification number LMT/BRAVO/2026-13**)**

1. This specification describes the software product to be developed, the purpose of which is to collect medical information and data from sensor devices, perform their validation, storage, organization, and processing in the context of other data (linearly and using AI algorithms) and organizing access to external systems, providing a cloud-based platform (developing a new platform or adapting an existing one) as a service for conducting medical research related to breath analysis.
2. The bidder shall submit a Technical Proposal in accordance with the open tender announced by AS "LabMedTech" for the procurement titled "Development of cloud-based software, including a database, analyses, and other functionalities" (identification number LMT/BRAVO/2026-13) the requirements of the Tender Documents and Technical Specifications, with the Technical Proposal providing a detailed description of the fulfillment, provision, and implementation of all requirements, including all activities related to development, delivery, and warranty technical support, which will result in the implementation of the subject matter of the procurement. The description must be sufficiently detailed to assure the Contracting Authority of the Bidder's ability to fulfill all requirements set forth in the Tender Regulations and the Technical Specifications.

TECHNICAL REQUIREMENTS / SPECIFICATIONS:

Development/Delivery/Warranty Technical Support*	**Quantity**	**Unit**	**Requirements**
1. Base platform for a cloud-based solution for conducting medical research	1	Platform	● **Location and Compliance:** The platform must be located in the European Union (EU) and must strictly comply with GDPR and HIPAA data protection requirements. ● **Data Processing and Performance:** The platform must be capable of receiving data, performing real-time or near-real-time data analysis, and conducting quality control with anomaly detection. It must ensure drift compensation, signal data normalization in response to environmental changes, and the harmonization of multiple instruments. ● **Architecture:** The solution must be implemented as a multi-tenant web application based on microservices architecture and container orchestration. All services must be containerized and stored in a centralized container registry. ● **Data Storage:** Core transaction and configuration data must be stored in a managed relational database. Large volumes of sensor and log data must be stored in a scalable object store, while a specialized time-series database must be used for time-series queries. ● **Security and Encryption:** All data traffic must be encrypted. For external data traffic, TLS termination must be used on the load balancer or API gateway. For data that has not been accessed for an extended period (at rest) in databases, object stores, and attached storage, managed encryption with a key management

			system must be used. ● **Access Control and Monitoring:** A centralized identity management system with role-based access control must be used for authentication and authorization. The platform must implement appropriate activity logging, metrics, and system monitoring using centralized auditing and security posture monitoring tools to detect incidents and threats. ● **Portability:** The platform must be made available to the client upon project completion and must be designed so that it can also be deployed on the Client's server (as a containerized solution). The Client must be able to independently use the data for model training and integrate their own data processing algorithms developed in *the Python* environment.
1.1. Secure, automated data exchange	1	Module	● **Encryption and security:** Data transmission functionality must be provided with mandatory encryption in transit (at least AES-256 and TLS 1.3 standards) and encryption at rest. ● **Data exchange mechanisms:** The module must expose RESTful or equivalent API endpoints. Event-driven integration with asynchronous delivery and message buffering must be provided for reliable decoupling. The RESTful API must allow respiratory analysis instruments to upload new measurement data. ● **File Transfer:** Standard protocols (e.g., SFTP) must be supported for secure file transfer from medical devices or partners. ● **Management:** API keys, certificates, and accreditation data must be stored in a secure secrets management system. Access control must be integrated with the API gateway. All access and configuration changes must be logged in audit logs and linked to an automated threat detection system in accordance with healthcare and GDPR requirements. The vendor must provide incident response plans in accordance with GDPR and HIPAA.
1.2. Data preprocessing, scaling, transformation, database	1	Module	● **Signal processing logic:** The module must implement preprocessing of time series and other data types for the analysis of respiratory analysis instrument data. Respiratory analysis instrument data must include measurement parameters, auxiliary data (e.g., environmental and instrument conditions), as well as sensor response data from multiple sensors. The signal processing pipeline must be configurable and extensible so that new instruments with varying data structures can be added later. The signal processing pipeline must include determination of the measurement period and exhalation phase, visualization of the sensor baseline, normalization, and calibration (to compensate for fluctuations in temperature, humidity, and pressure, as well as sensor aging). ● **Error Detection:** Detection of erroneous signals (e.g., noise, excessive peaks) and feature extraction (delta normalization, exhalation characteristics) must be ensured. ● **Data Pipelines:** Preprocessing must be implemented using scalable data transformation tools that operate within a data lake with a centralized data catalog.

			• **Instrument Calibration Data**: Must be stored in the system and appropriately integrated into the data stream. Calibration data may include reference measurements. A dedicated calibration pipeline must be implemented to derive calibration parameters from calibration measurements, thereby reducing the impact of drifts, sensor aging, cross-talk, and device variations. • **Data Storage Formats:** Processed and historical data must be stored in an object store in optimized, encrypted formats (e.g., CSV or JSON). A relational database should be used for structured queries, while a time-series database should be used for time series data ( ). • **Data Governance:** Data access and schema evolution must be strictly controlled by a data governance layer, ensuring that users see only authorized data. Automated detection of sensitive personal data must be implemented in both raw and pre-processed layers.
1.3. Data Analysis and Model Development	1	Module	• **Analytical Functionality:** The module must implement mathematical, statistical, and machine learning (ML)-based data analysis (including neural networks) to generate predictions and determine disease classifications. Analysis of features and their impact must be provided. • **Machine Learning (ML) Platform:** A unified, managed ML platform must be used for data exploration, development, and collaboration in model development. Managed training processes must be provided using built-in algorithms or custom containers. • **MLOps and Governance:** Experiment tracking, model version management (registry), and analysis of model explainability and bias for medical purposes must be implemented. Automated ML pipelines must be used for repeatable workflows. • **Infrastructure Monitoring:** All operations, compliance/control evidence, and metrics must be automatically routed to a centralized logging and audit system.
1.4. Deployment of the model for use by researchers and healthcare professionals	1	Module	• **Deployment Architecture:** Developed models must be hosted and deployed in a scalable environment managed through an API gateway. Access must comply with GDPR and HIPAA requirements. • **Network Security and Integration:** Network access to model endpoints must be restricted using virtual private networks (VPNs), security groups, and private links, ensuring a secure connection to hospital and research networks. • **Monitoring:** The system must monitor performance metrics (latency, error rate, throughput) in real time and detect data and model drift. All API calls must be logged with full traceability in audit logs.
1.5. Interface for data browsing and research	1	Module	• **User Interface (UI):** Researchers and physicians must be provided with a secure web application that is globally accessible with low latency and protected by a web application firewall (WAF). • **Functionality:** The interface must support data browsing, report generation, result visualization, and data

			aggregation based on group membership and measurements. Business intelligence (BI) or interactive analytics dashboards must be integrated for information presentation. ● **Different user types require different user interfaces**: User types include administrators (who can perform backups, updates, and user management), clinicians (doctors, nurses) with access to data about their patients and the ability to upload new measurements, and researchers with the ability to access datasets and configure/implement data analysis workflows. ● **Access and Control:** Authentication and authorization must use a centralized solution with role- and attribute-based permissions (RBAC/ABAC). All user interface actions, particularly data export and access, must be logged and retained for audit purposes.
1.6. Platform module for patient metadata collection and consent management	1	Module	● **Database and Security:** Patient metadata and consent records must be stored in an isolated database with strict network controls and encryption. ● **Architecture:** Data entry and editing logic must be implemented as microservices behind an API gateway. ● **Privacy and Compliance:** Immutable audit logs must be created for all data subject rights actions (access, correction, deletion) and consent changes. The system must provide an interface where an individual gives active consent for data operations. All personal data across all datasets must be stored and processed in a manner that ensures protection in accordance with the GDPR and HIPAA frameworks.
1.7. Adapting the platform to handle new data types (GC and MOX integration)	1	Updated platform	● **Scalability:** The platform must be capable of assimilating additional data modalities, such as gas chromatography (GC) and metal oxide (MOX) sensor readings. GC data ingestion, peak detection, and correlation must be ensured. ● **Data pipelines:** New data processing and ingestion logic must be implemented as automated data processing jobs that operate on data stored in the object storage and are managed through a central data catalog. ● **Big Data Analytics:** Time-series features and spikes must be stored in relational or time-series databases. Large-scale multimodal feature sets should be stored in an optimized format, enabling high-performance SQL queries using analytical data warehouses or query tools. ● **Multimodal modeling:** To combine GC-derived and MOX sensor features, monomodal and multimodal models must utilize a unified MLOps lifecycle (training, experiments, pipelines, and registry) within a centralized ML platform. ● **Visual Analysis:** Integrated visual analysis of chromatograms, GOS profiles, and sensor signatures must be accessible via an API and displayed in secure, embedded dashboards. All access to both data modalities must be centrally auditable and protected.

Name and surname of the bidder or its authorized representative _____
Position _____

The date of signing of this document is the date of the attached secure electronic signature and its timestamp.
The bid (including this document) shall be signed by the bidder's representative with a secure electronic signature and a timestamp.