**MIECS Privacy Notice - Data Protection and Confidentiality**

**Version 1.0 31/05/2022**

**What is the MIECS database?**

The MIECS database is the repository of data collected from patients participating in the MieCS study conducted by the Special Unit for Biomedical Research and Education (SUBRE) of the School of Medicine of AUTh. The information in the database will be used to compare different types of heart and lung machines in patients undergoing cardiac surgery.

**What information does it contain?**

The information includes demographic details about the participating patient, their medical history, their postoperative progress, clinical data, and lab & paraclinical examination results.

**What is the legal basis for the MIECS database?**

MIECS data are collected based on the informed consent of the participants as defined in Art. 6(a) EU 679/2016 (GDPR) and Greek law 4624/2019, for the promotion of scientific knowledge and the improvement of healthcare.

**Who manages the MIECS database?**

The MIECS database is managed by the Clinical Research Unit of SUBRE, School of Medicine, AUTh and Dendrite Clinical Systems, our technology partner.

**What happens to the data and who can see it?**

The data are collected by the study official after the operation on the participating patient. Hospital computers are used to collect the information, which is collated, checked, and approved before being uploaded to the database under a study ID. The information uploaded to the database does not include names or contact information. Only an approved member of the study officials can load the data onto the MIECS database. Once the records have been loaded, they can be reviewed by authorised staff of the study using an approved user account with a secure password.

When the data have been checked and confirmed by the study official, the software engineers and data analysts at Dendrite Clinical Systems will download the data to a secure server in Dendrite’s offices.

The data will not be shared with anyone outside the study centres or used for purposes other than those specifically mentioned during the informed consent procedures. At the end of the three year and a half contract period, 1/12/2025, the MIECS data will be deleted or securely transferred to a new provider.

**MIECS Database Server**

The server is hosted within a data centre in London, by RackSpace. This is a tier four data centre which meets the highest levels of building security.

The service delivery and information governance provided complies with ISO 20000 & ISO 9001 accreditation and the security structure is aligned alongside ISO27001. The security arrangements are internally audited approximately every three months and externally audited every six months.

All servers have firewall and anti-virus software installed which is configured to use real-time scanning.

## Backup Resilience

The data is securely backed-up each day. All backed up data stored is compressed, de-duplicated and encrypted within a secure off-site vault.

There are two backup vaults, the primary one is hosted locally and is then backed up to a secure secondary off-site vault hosted within a separate datacentre located at Heathrow.

**Dendrite Security**

Dendrite Clinical Systems is assessed against NHS Information Governance standards, which includes both physical and organisational security measures. Dendrite’s toolkit assessment score is available on the IG Toolkit website (https://www.dsptoolkit.nhs.uk/OrganisationSearch/8HJ38).

The computer software program created by Dendrite that holds the MIECS data has been independently tested to ensure that it is not vulnerable to unauthorised access, or internal breaches of security.

**Can I ask to see the data that the MIECS registry holds about me?**

Requests to see what data is held on the MIECS database about you may be made via contacting the study coordinator at papazisg@auth.gr or other study officials as mentioned in the Participant Information Sheet.