

Appendix 4: Data Security Policy

Public reference copy of Appendix 4. Annex 1 containing detailed technical and organisational security measures is withheld from this public copy; it remains part of the signed Agreement.

This Data Security Policy forms an integral part of the EURO-NMD Registry Data Sharing Agreement (the “Agreement”) and describes the technical and organisational measures implemented to protect the confidentiality, integrity, availability, and resilience of Registry Data.

This Policy complements Article 7 (Security Measures) and Article 21 (Data Access) of the Agreement and applies to all Parties participating in the EURO-NMD Registry, including the Coordinator, the Registry Host, Consortium Members, and participating Healthcare Providers (HCPs).

The objective of this Policy is to ensure that Registry Data are processed securely and in compliance with applicable Data Protection Legislation, including the General Data Protection Regulation (GDPR), and to establish a common framework for information security across the Registry.

All Parties shall implement and maintain appropriate technical and organisational measures to protect Registry Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, unauthorised access, or any other form of unlawful Processing.

1. System Hosting

- The Registry Database is hosted and maintained by the University Medical Centre Freiburg (UKLFR).
- The Registry is implemented using REDCap, a secure web-based electronic data capture platform developed by Vanderbilt University.
- The hosting environment includes appropriate technical and organisational safeguards, including access controls, system monitoring, backup procedures, and redundancy mechanisms designed to ensure the confidentiality, integrity, availability, and resilience of Registry Data.
- The Registry infrastructure is operated in accordance with applicable Data Protection Legislation and institutional information security requirements.

2. Pseudonymisation and Personal Data Protection

- All Patient Data entered into the Registry must be pseudonymised by the contributing HCP prior to submission to the Registry.
- Each Patient is assigned a unique Registry identifier within the Registry Database.
- The patient re-identification key linking the Registry identifier to the identity of the Patient shall remain exclusively under the control of the contributing HCP and shall never be transmitted to, or stored within, the Registry.
- The Registry does not collect directly identifying data such as patient names, personal email addresses, postal addresses, or national identification numbers.
- Limited demographic and clinical information necessary for the purposes of the Registry may be processed, including date of birth, sex, and health-related data, as further described in the Registry Data Dictionary.
- Where Registry Data are disclosed to authorised Recipients, additional data minimisation and pseudonymisation measures shall be applied in accordance with the Data Access Policy.

3. Data Transmission and Storage

- Registry Data transmitted to or from the Registry Database shall be protected using industry-standard encryption protocols, including SSL/TLS encryption.
- The Registry Host shall implement appropriate technical and organisational measures to protect Registry Data, including access controls, firewalls, malware protection, system monitoring, and vulnerability management.
- Backup copies of the Registry Database shall be performed regularly, retained for a minimum period of ninety (90) days, and stored separately from the production environment.
- The Registry infrastructure shall be operated in a manner designed to ensure the availability, integrity, and resilience of Registry Data and services.

4. User Access and Authentication

- Each User shall be assigned an individual, non-transferable, and non-shared user account approved by the Principal Investigator or authorised representative of the relevant HCP.
- Access to the Registry shall be restricted through authentication mechanisms and role-based access controls, in accordance with the principle of least privilege and the Data Access Policy (Appendix 6).
- Access rights shall be limited to those necessary for the performance of the User's authorised functions.
- Export, extraction, or download of Registry Data by Users shall be permitted only where authorised under the applicable role-based permissions defined in the Data Access Policy.
- The Registry shall maintain audit logs recording relevant user activities, including user authentication events, data exports, and modifications to Registry Data.
- User accounts shall be reviewed periodically and deactivated, suspended, or removed without undue delay where access is no longer required.
- The Registry Host shall implement session management, audit logging, and other technical safeguards proportionate to the risks associated with the Processing.

5. Confidentiality and Accountability

- Personnel of the Registry Host and the Coordinator may access Registry Data only to the extent strictly necessary for system administration, maintenance, security, technical support, legal compliance, or other authorised purposes under the Agreement. Such access shall be logged where technically feasible.
- Each HCP and its authorised Users remain responsible for the accuracy, completeness, lawfulness, and quality of the HCP Data submitted to the Registry.
- Personnel of the Registry Host and the Coordinator with access to Registry Data shall be bound by confidentiality obligations, whether through employment contracts, institutional policies, confidentiality undertakings, or equivalent legally binding arrangements.
- The Registry Host and the Coordinator shall maintain documented procedures for security incident management, including the detection, reporting, investigation, mitigation, and notification of Personal Data Breaches in accordance with the Agreement and applicable Data Protection Legislation.

6. Third-Party Access (Recipients)

- Recipients may receive access only to Aggregated Data or Pseudonymised Registry Data, subject to approval by the Data Access Committee (DAC) and in accordance with the Agreement and the Data Access Policy (Appendix 6).
- Any disclosure of Registry Data to a Recipient shall be subject to an appropriate legal agreement, including where applicable a Data Transfer Agreement, Data Access Agreement, or equivalent contractual arrangement specifying the permitted use, duration, security requirements, and other applicable safeguards.



- Any attempt to re-identify Patients or to use Registry Data for purposes outside the scope approved by the DAC is strictly prohibited.
- Where Registry Data are disclosed to commercial entities, only data relating to Patients who have consented to such use may be shared, in accordance with the informed consent provided and the Data Access Policy.
- Recipients shall not directly contact Patients or attempt to recruit Patients using Registry Data. Any approved patient contact or recruitment activity shall be conducted exclusively through the treating HCP and in accordance with the Agreement and the Data Access Policy.

7. Governance and Compliance

- Each HCP shall obtain and maintain all approvals, authorisations, ethics committee approvals, and other governance approvals required under applicable national, institutional, and regulatory requirements before contributing data to the Registry.
- The Processing of Patient Data within the Registry is based on the informed consent of the Patient or, where applicable, their legal representative. Each HCP is responsible for obtaining, documenting, and retaining valid informed consent prior to entering Patient Data into the Registry, in accordance with Article 6 of the Agreement.
- In accordance with Article 10 of the Agreement, the Coordinator has conducted a Data Protection Impact Assessment (DPIA) for the Registry processing activities. Each HCP shall assess, in consultation with its Data Protection Officer and in accordance with applicable national and institutional requirements, whether it is required to conduct an additional DPIA in relation to its own Processing activities.
- The Registry shall be operated in accordance with the Agreement, applicable Data Protection Legislation, the Governance Rules, the Data Access Policy, and other Registry policies adopted by the Steering Committee.
- This Policy shall be reviewed periodically and may be updated to reflect changes in applicable legislation, security requirements, Registry operations, or recognised best practices. Any material updates shall be communicated to participating HCPs and other relevant stakeholders.

