EURO-NMD
Registry Hub
European Reference Network
for neuromuscular diseases

DATA SECURITY POLICY

This policy describes the data security measures incorporated in the EURO-NMD Registry, including the collection, use of and access to data, all of which are conduct in full compliance with the European General Data Protection Regulation (GDPR)[1] and national laws and regulations pertaining to data protection and data privacy.

The EURO-NMD Registry is a patient registry for all rare, paediatric and adult, neuromuscular diseases. It is a pan-European, collaborative effort led by EURO-NMD, an ERN for the thematic grouping of rare neuromuscular diseases, to build the first unified NMD Registry in the EU.

The purpose of the EURO-NMD Registry is to improve the quality of care and outcomes for NMD patients across Europe, while providing sufficient data to launch research and clinical trials, inform policy and regulatory decisions.

The Registry received funding from the 3rd EU Health Programme and was jointly developed by a consortium of organisations: · Assistance Publique–Hôpitaux de Paris (AP-HP), · University Medical Centre Freiburg (UKLFR), · Radboud University Medical Center (Radboudumc), · World Duchenne Organization (UPPMD), · Duchenne Data Foundation (DDF), · Institute of Myology (AIM), · French Muscular Dystrophy Association (AFM-Téléthon).

The EURO-NMD Registry is a registry maintained on REDCap, a web-based database developed by Vanderbilt. The REDCap server is housed in a secure central facility of the University Medical Centre Freiburg (UKLFR) and maintained by UKLFR IT staff.

All data transmitted to, or extracted from, the registry platform is protected using SSL/TLS encryption. The registry platform limits personally identifiable data to Patient's Date of Birth, Gender, information about their clinical and genetic diagnosis and the name of their treating centre of care, other potential identifiers, including, but not limited to, Patient Name, Patient Email Address, or National Identification Number, are not part of the registry.

Access to the REDCap server is password-protected and passwords are encrypted, and can only be accessed by approved registry staff who sign a Confidentiality Agreement whereby they undertake to maintain the confidentiality of any data that they access in the Registry.

Hospitals and users of the registry are responsible and liable for all data which they submit into the online system and must ensure compliance with all relevant ethical and privacy standards. To access the online database, hospital users must be affiliated to a centre part of the EURO-NMD network of healthcare providers and have an approved user account, which requires explicit approval by the principal investigator of the involved centres. In addition, hospitals must obtain approval by their relevant national or local governance authority and ethics committee to participate in the registry and

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

This document is part of the project 'EURO-NMD Registry' co-financed by the European Commission under the Third Health Program (grant agreement 101055286). The EURO-NMD Registry has also received funding for 5 months from the EU4health program (grant agreement 101085084) and will continue to be funded for the 2023-2027 period under the call EU4H-2023-ERN-IBA.

have an agreement with the registry establishing the terms of participation including, but not limited to, the requirement to obtain consent for data processing and to apply pseudonymization before entering any data into the registry. The re-identifying key is kept at the local site and securely stored in such a way that re-identification of individuals is only possible by clinicians caring for patients.

Hospital staff shall transfer data to the Registry central database by entering data manually on associated data entry forms or by importing data from CSV (comma-delimited) files via the REDCap user interface. Variables are entered according to the guidance provided in the EURO-NMD Registry Data Dictionary. The initial data collection occurs at routine clinical visits and follow up data of participants are updated annually. Data are entered longitudinally and for each visit a set of data entry forms, consisting of a minimal dataset which is common across all diseases and sites, are presented. Hospital staff can only enter required information into the EURO-NMD Registry web tool.

Information held by the Registry is confidential, and access to data is restricted based on user role. A hierarchical access authorization system is implemented and web access is only provided at an individual level using two-step verification protected user accounts. All requests for local user accounts must be approved by the hospital Coordinator/representative from the same organisation on behalf of which the user is requesting access. Only authorized users at hospital sites will have direct access to the Registry and they can only access data from patients treated at their own site. Hospitals can use the online tool to produce summary data reports, export data for local analysis, and monitor and compare their performance to other participating hospitals.

The procedure for making a request for data by a third party is outlined more extensively in the EURO-NMD Registry Data Access Policy. In summary, data access request by third parties are made in writing through an online Data Access Request Form. Only pseudonymized or aggregate data can be provided to third parties on approval by the Registry's Steering Committee and/or the Data Access Committee (DAC). Data is provided to applicants for approved studies only after the approval processes have been met and a Data Transfer Agreement has been signed.

Provision of data for linkage studies and commercial purposes is only possible if patients have specifically given permission for their pseudonymized data to be shared and combined for those purposes. Likewise, requests seeking to use the Registry to recruit participants for other relevant research projects may be met, where registrants have consented to being contacted again for this purpose. Consenting registrants will be contacted by their treating clinician. Registrant contact details are not released to researchers.

The registry is based on Consent. However, to confirm compliance with the principles set forth in article 35 of GDPR, the Coordinator, on behalf of the Members of the Consortium, completed a Privacy Impact Assessment (PIA) for the Registry database. This document is kept on file and will be reviewed regularly together with this Data Security Policy to ensure compliance with newly ratified legislation or institutional policies. Any changes will be communicated to all hospitals using the Registry platform, as well as authorized users, and other relevant stakeholders.

Data Security Measures for the European Registry for Rare Neuromuscular Diseases (EURO-NMD Registry)	
- *Measures of pseudonymisation and encryption of personal data:*	- *pseudonymisation is not part of the EURO-NMD Registry. A patient ID is generated automatically by the REDCap-system. Allocation lists for patient ID – name are not part of the REDCap-database of this project and must be stored separately.*
- *Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services*	- *Confidentiality: All data access is done using authentication and authorization. Each HCP user can only access patients from his/her own site (REDCap Data Access groups)* - *Integrity:* - *SSL-certificate proves identity of REDCap-system and protects data transfer* - *REDCap Logging-Module lists all changes made to this project, including data exports, data changes, and the creation or deletion of users* - *Availability and resilience: System is hosted in a redundant computer center and monitored (alerts for system offline, high CPU usage, high memory usage, disk space).*
- *Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident*	- *90 days backup for the whole virtual machine that hosts the REDCap-system and for individual files / all data on the system. Backups are physically separated from the runtime environment.*
- *Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing*	- *General yearly testing of restoring data from backup*

This document is part of the project ‘EURO-NMD Registry’ co-financed by the European Commission under the Third Health Program (grant agreement 101055286). The EURO-NMD Registry has also received funding for 5 months from the EU4health program (grant agreement 101085084) and will continue to be funded for the 2023-2027 period under the call EU4H-2023-ERN-IBA.

- *Measures for user identification and authorization*	- *users have to apply for an account on the system. ERN coordinator approves requests. Once approved, accounts are set up in REDCap. Expiration date, password rules, account deactivation after too many incorrect login-attempts or inactivity, separate authorization on project-level (Roles, Data Access Groups)*
- *Measures for the protection of data during transmission*	- *SSL-encryption*
- *Measures for the protection of data during storage*	- *Controlled access to REDCap-database only for authorized and trained personnel* - *antivirus* - *firewalls* - *intrusion detection* - *weekly and on-demand system- and software-updates*
- *Measures for ensuring physical security of locations at which personal data are processed*	- *stored in university hospital computer center which complies to german KRITIS-Verordnung for critical infrastructure*
- *Measures for ensuring events logging*	- *event-logging is automatically done by REDCap-system*
- *Measures for ensuring system configuration, including default configuration*	- *only REDCap LTS versions* - *system changes are documented* - *installation protocol and configuration checks*
- *Measures for internal IT and IT security governance and management*	- *IT is managed in compliance with University Medical Center IT standards (regular meetings, regulated responsibilities, security operations team at university medical center Freiburg)*
- *Measures for certification/assurance of processes and products*	- *Clinical Trials Unit Freiburg is a certified ECRIN-datacenter*
- *Measures for ensuring data minimization*	- *usage of Key Performance Indicators to ensure that all data items collected will be used in data analysis*

This document is part of the project 'EURO-NMD Registry' co-financed by the European Commission under the Third Health Program (grant agreement 101055286). The EURO-NMD Registry has also received funding for 5 months from the EU4health program (grant agreement 101085084) and will continue to be funded for the 2023-2027 period under the call EU4H-2023-ERN-IBA.

- *Measures for ensuring data quality*	- *REDCap data quality rules for live plausibility-checks and warnings for implausible values* - *datatype-validation* - *branching-logic* - *use of standardized instruments / CRFs*
- *Measures for ensuring limited data retention*	- *registry design has been curated by domain-experts and cleaned / harmonized afterwards so that only information relevant for the project-purpose is being collected*
- *Measures for ensuring accountability*	- *Clinical Trials Unit Freiburg has procedures for data protection related issues (SOPs, rules for data breaches, data protection officer)*
- *Measures for allowing data portability and ensuring erasure*	- *data and metadata can be exported in multiple widely used formats (PDF, CSV, R, SPSS, SAS, CDIDC / XML, turtle, owl,…)* - *data erasure is possible for registry users directly in the REDCap-system; complete data removal from backups as well automatically after 90 days*
- *For transfers to (sub-) processors, also describe the specific technical and organizational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter*	- *no sub-processor defined yet* - *data transfer is generally done via controlled procedures (data encryption, use of local cloud-platforms)*

This document is part of the project 'EURO-NMD Registry' co-financed by the European Commission under the Third Health Program (grant agreement 101055286). The EURO-NMD Registry has also received funding for 5 months from the EU4health program (grant agreement 101085084) and will continue to be funded for the 2023-2027 period under the call EU4H-2023-ERN-IBA.