MSBASE FOUNDATION
DATA SECURITY & GOVERNANCE

The MSBase and MGBase registries are operated by the MSBase Foundation (MSBF) – a not-for-profit organisation with 20 years' experience in facilitating collaborative, global research in multiple sclerosis and other neuro-immunological diseases, and which has developed a comprehensive, globally accepted governance framework for international data sharing. Participating neurologists contribute pseudonymised patient data collected at their centre during routine clinical care to the registry via the freely available iMed Web application, and in turn, can request access to the global dataset to conduct research on approved projects.

Good governance

- The MSBase Foundation does not own the data contained in the registries. The MSBF is considered a processor of the centre's data.
- The centre is the owner of all their data and can request to withdraw data from the registry at any time.
- Principal Investigators choose how their centre data is used and can opt-out of any investigator-initiated project requesting access to the global dataset.
- Centres must follow their applicable data protection legislation when sending and receiving data from the registries to conduct research.
- The Principal Investigator must also agree to and sign a Data Use Agreement to receive data for analyses.

Data security - Centre (online)

- iMed Web is a web application that provides secure, browser-based access — enabling faster deployment and seamless updates.
- Azure SQL is used for data storage, encrypted with TDE, and constrained to the local region to maintain data sovereignty
- Access managed through Azure Front Door, providing a WAF and geo-restriction.
- iMed Web supports Microsoft Entra ID Single Sign-On (SSO) via OpenID Connect (OIDC), enabling secure, standards-based authentication with streamlined user access, centralised identity management, and improved security through reduced password exposure. You may enforce conditional access to comply with your own security requirements. Addiitonal authentication providers may be added in the future.

Data security - Registry

- The Registry data is hosted in Microsoft Azure using multilayered, built-in security controls. The SQL Database is encrypted using Azure's Real Time SQL Transparent Data Encryption (TDE).
- Azure Front Door, Firewalls and Geo-blocking protect data from cyber attacks.
- The Azure SQL Database meets regulatory compliances such as ISO/IEC 27001 & FedRAMP/FISMA and SOC and PCI DSS.
- MSBase Foundation systems are subjet to yearly penetration tests by an external security specialist.

Patient confidentiality

- A centre's patient data is physically isolated. Every centre has their own dedicated URL and database eliminating risks of cross centre patient access.
- Only records from consented patients are shared with the registry.
- Data is pseudonymised before it is shared with the registry - in this process, identifying information such as name and address are removed, a patient code is used to communicate without exposing any patient Personally Identifiable Information (PII).

ISO 27001 certified

- As a not-for-profit organisation supporting global research and clinical collaboration, we recognise the responsibility that comes with managing sensitive research and operational information.
- The MSBase Foundation is proud to be ISO/IEC 27001 certified, demonstrating that our Information Security Management System (ISMS) has been independently assessed against an internationally recognised standard.

MSBase Neuro-Immunology Registry

MGBase Myasthenia Gravis Registry