MSBase
Neuro-Immunology Registry

Quick guide to MSBase Registry data governance and security

The MSBase Registry is operated by the MSBase Foundation – a not-for-profit organisation with 20 years' experience in facilitating collaborative, global research in multiple sclerosis and other neuro-immunological diseases that has developed a comprehensive, globally accepted governance framework for international data sharing. Participating neurologists contribute pseudonymised data to the registry via one of two freely available software applications, MDS and iMed, and in turn, can request access to the global dataset to conduct research on approved projects.

Good governance

- MSBase does not own the data contained in the Registry. The registry is considered a processor of the data.
- The MSBase 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 when receiving data from the MSBase Registry to conduct research.
- The Principal Investigator must also agree to and sign the MSBase data use agreement to receive data for analyses.

Data security - centre level

- Each Centre is responsible for ensuring adequate security measures are in place to secure their confidential patient data stored at the local level in accordance with their applicable IT/security policies and all applicable laws in their jurisdiction.
- Principal Investigators are responsible for assigning their centre staff with the required levels of authority in the iMed/MDS application.
- MSBase Registry staff do not have access to identifiable centre data.

Patient confidentiality

- No patient identifiable information (PII) is shared with the registry – only sex and month and year of birth are collected. PII is stored at the local level only.
- Data is pseudonymised *before* it's shared with the registry – in this process, identifying information such as name and address are removed and each patient is assigned a hexadecimal code called a "Globally Unique Identifier" (GUID).

Data security - registry level

- 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).
- The Azure SQL Database meets regulatory compliances such as ISO/IEC 27001 & FedRAMP/FISMA, SOC and PCI DSS.
- Centres also have visibility of their own patient data within the registry. Patient records cannot be changed in the registry (read only).

Click **here** to view the complete MSBase Foundation governance package on the MSBase Registry website.