

## MiNDAUS Privacy Policy

Policy Number	PP-001	Version	1.2
		Date approved	09 Oct 2025
Person responsible	Professor Steve Vucic	Scheduled review date	1/10/2026

The MiNDAUS Leadership Group endeavours to deal with personal information in accordance with the Australian Privacy Principles.

Personal information is information or an opinion that identifies or could reasonably identify an individual.

### Purpose

The purpose of this Privacy Policy is to summarise how the MiNDAUS Patient and Clinical Registry deals with personal information.

### Background

The MiNDAUS Registry collects and handles personal information in order to carry out its activities.

### Technological Security

TRRF uses Django 4.2 (upgrading to 5.2), the latest LTS (Long term support) release of Django. LTS releases get security and data loss fixes applied for a guaranteed period (3+ years). Django itself provides distinct levels of built-in security including SSL (Secure Socket Layer) security with all web traffic to and from application encrypted; CSRF (Cross-Site Request Forgery) checking making impossible man in the middle attacks (falsifying form submissions for example); and Login restrictions of all “views”. Access to the front-end is via an SSL configured web server with an up-to-date cipher suite which provides perfect forward security, reducing the consequences of a compromise of the server SSL key, while also allowing use of ciphers which increase client performance. Web-Application-Firewall, using Cloudfront and S3 Virus Scanning has also been introduced to TRFF as enhancements.

TRRF itself includes a fully configurable permissions layer (role-based security model) which restrict the visibility of forms (and fields) to specified user groups. Furthermore, TRRF stores identifying patient contact/demographic data in a totally distinct database to any clinical/genetic data. The servers and related infrastructure are maintained by Amazon Web Services (AWS), where the risk of unauthorised access, tampering or theft is reduced to a minimum.

The architecture of the system uses AWS Fargate managed service structures, including serverless technology to increase security and reduce operational overheads and risk. Advanced security protection is built into the infrastructure including web application firewall, guard duty threat detection, centralized application and audit logging, and data encryption at rest and in transit. The system is also subject to external security testing and audit. Secure data management practices ensure sensitive patient data is masked when undergoing external testing. The database these systems use is encrypted, which ensures

# MiNDAUS PARTNERSHIP

that data is protected if the storage hardware is (for example) stolen, reused, or returned to the manufacturer to address a fault.

Communication between the front-end and the databases is encrypted. This is to guard against confidential data being intercepted “in transit”. In addition to encryption, SSL certificates are used (and databases and database clients configured to verify them) so that a third party cannot impersonate the database or a database client.

## Collection of personal information

The MiNDAUS Registry collects personal information from participants who have given informed consent, and from Healthcare Professionals involved in their care.

The types of personal information the MiNDAUS Registry collects include:

- contact details (for example, name, address, professional information, telephone numbers and email)
- demographic information (for example, gender and date of birth)
- professional information (for example, job, education) and
- activity-related information (attendance at Specialist MND clinics, other healthcare appointments and participation in any research).

In conducting its activities the MiNDAUS Registry will collect health and other sensitive information. For example, the MiNDAUS Registry collects medical history information from patients and may also access data from other sources about them with their written and informed consent.

The MiNDAUS Registry collects personal information directly from individuals in the following ways:

- from people with MND, or their family carer entering their own information
- electronically through clinical documents and online surveys
- from forms and other correspondence (including electronically)
- during telephone calls
- during Telehealth Consultations
- while delivering and administering services and
- face to face contact.

## Purpose of Collection and Use

The MiNDAUS Registry collects personal information as required to carry out one or more of its functions or activities, including:

- to improve communication between people with MND, their family carers, the Specialist MND Clinics and community healthcare providers and primary care.
- to provide a national repository for MND key clinical milestones, disease progression measures, service use and treatment use;
- to enable services to compare their practices and outcomes to others around Australia;
- to inform the need for continuing professional development, education and training for Health Professionals involved in MND care.

# MiNDAUS PARTNERSHIP

- to enable planning, policy and service development.
- to promote to participants appropriate research opportunities for which they may be eligible.

## Sensitive Data Practices

The MiNDAUS Patient Registry collects fully identifiable personal information with the consent of individuals or their legal guardian using an online portal of TRRF that is accessible through a two-factor password protected secure login. The persons entering their data have full control over what is entered and can update it at any time or put in a process for deletion of the records if they choose to withdraw from the Patient registry. The individual will be given the option to consent to link their personally entered data with that of the Clinical Registry. The Office of eResearch team will perform quality assurance processes on records to identify potential errors or missing data.

The MiNDAUS Clinical Registry also collects fully identifiable personal information with the consent of individuals or their legal guardian using an online portal of TRRF that is accessible through a two-factor password protected secure login. Those entering clinical data will be nominated by the Site Principal Investigator and provided comprehensive training.

At any point, patients can withdraw their permission for further data collection and participation. The Data/Operations team will act as Data Custodian and perform quality assurance processes on records to identify potential errors or missing data, in association with The Office of eResearch team.

## Disclosure

The MiNDAUS Registry only discloses personal information for the primary purpose for which it was collected, or for a secondary purpose as required or permitted by law.

For example, the MiNDAUS Registry may disclose personal information to third parties it engages to assist it in performing its functions, most often related to enhancing clinical services and for research purposes. Where disclosure takes place the MiNDAUS Registry aims to include protective provisions regarding the handling of personal information in contracts with third parties.

When conducting a survey on behalf of a third party, the MiNDAUS Registry does not disclose personal information to that third party. When the MiNDAUS Leadership group has approved a future research project, personal information of eligible participants will not be disclosed to that third party. The MiNDAUS Registry will contact eligible participants with the details of the potential research and the participant will then contact the third party directly to express their interest.

# MiNDAUS PARTNERSHIP

## Website Privacy Statement

### Your privacy and confidentiality

We will keep any information confidential and securely stored. We will use and retain information that we collect about you for this project, and with your permission store it in the MiNDAUS Registry.

The MiNDAUS Registry is a secure platform that allows data collection which can also be used to share the data with other researchers, as approved by the MiNDAUS Leadership Group, to maximise the benefit of the project in alignment with the Australian Government's Open Access Policy. If third parties are given access to your data, their databank must provide the same level of data security and protection of your privacy and confidentiality as for this project.

Neither we nor they will disclose your personally identified information without your permission, except in compliance with the law. Where we transfer your data to approved collaborators we will do so in a format where you are not identifiable to anyone under normal circumstances. What this means is that your data will be functionally anonymous if intercepted. However, we will attach a code to it so that we will be able to link it back to you. The files that allow us to break the code are held in a secure and separate place and are password protected so it is highly unlikely that anyone could gain access to your information. No personal information about you, such as your name and address will be shared with anyone outside of your recruiting site or an authorised member of the research team or the databank custodian and their staff.

All of your collected information will be kept for at least 10 years after the end of the study. We may keep the information for longer than the minimum period if it remains useful for research. Australian privacy law gives you the right to request access to your information that has been collected and stored. The law also gives you the right to request corrections to any information about you that you disagree with. Please contact the team using the details on the final page of this document if you would like to access your information. With your permission your treating GP and/or other medical professional will be notified of your participation in this study and of any clinically relevant information.

### Cookies

A record of each visit to the MiNDAUS website is logged – this is a small data file known as a cookie. A cookie does not identify individuals personally, but it does identify computers. Browser setting can be adjusted to disable cookies.

The following information from cookies is recorded to compile statistical information about the use of the MiNDAUS website. It is not used for any other purpose.

- IP address and/or domain name
- Operating system (type of browser and platform)
- The date, time and length of visit to the MiNDAUS website
- Pages and resources accessed, as well as documents downloaded.

# MiNDAUS PARTNERSHIP

## Access and Correction

The MiNDAUS Registry takes all reasonable steps to maintain the accuracy of personal information it holds. Individuals are encouraged to contact the Data Operations Manager, MiNDAUS Registries if the personal information held is incorrect.

Participants in the MiNDAUS Registry clients can view their information collected in the Clinical Registry but cannot edit it. If a change is required, then participants can talk to Project Staff at the MND Specialist Clinic or their treating Neurologist.

## Complaints and concerns

Any concerns about the MiNDAUS Registry handling of personal information should be directed to the Coordinating Principal Investigator, Professor Steve Vucic. on Ph. 02 9767 8447. Professor Steve Vucic may require complaints to be submitted in writing. After the MiNDAUS Registry receives all the relevant information, it will endeavour to resolve the complaint as soon as reasonably practical.

The website of the Office of the Australian Information Commissioner (OAIC) is an additional source of information [www.oaic.gov.au](http://www.oaic.gov.au). If an individual is not satisfied with how the MiNDAUS Registry has handled their complaint, they may wish to contact the OAIC.

## Responsibilities

All MiNDAUS Partners, Project Staff and associated entities will adhere to the MiNDAUS Privacy Policy at all times.

## Related Documents

[Privacy Act 1988 \(Cth\) \(Privacy Act\)\\*](#)

[Australian Privacy Principles \(Office of the Australian Information Commissioner 2014\)](#)

# MiNDAUS PARTNERSHIP

## REFERENCES:

Office of the Australian Information Commissioner. (2014, 22/7/2019). "Privacy Principles Guidelines (combined 2019)." Retrieved 17 January, 2021, from <https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines>.