Australasian Dermatology Registry

AUSTRALASIAN DERMATOLOGY REGISTRY DATA SECURITY POLICY

VERSION 1.0 APRIL 2023

PURPOSE OF THE DATA SECURITY POLICY

This data security policy describes the data security measures for the Australasian Dermatology Registry. The registry security processes are in accordance with ethical, legal and best practice guidelines. This policy includes collection, storage, and access of registry data for reporting and research.

THE AUSTRALASIAN DERMATOLOGY REGISTRY (ADR)

The ADR collects demographic, diagnosis, treatment, and quality of life data on people treated for skin conditions at participating sites within Australia and New Zealand. The ADR is designed to improve the quality of care for people living with skin conditions by informing dermatologists of the efficacy and risks of current and emerging treatment, the risk factors for developing a skin condition, and the impact these conditions have on the quality of life of the patients. Participating patients consent to their inclusion in the ADR.

REGISTRY DATA COLLECTION

Registry data are collected through a secure web portal with registry participants, following their consent, entering their own patient information including demographics, family history, comorbidities and quality of life. Clinic staff will be entering clinician reported data items including disease severity and treatment.

ADR participants complete an online web form that will automatically populate the registry when completed. Registry participants are not provided with a login for the registry, instead the registry matches, via a participating site specific QR Code, the participant data to the registry using name, date of birth and treatment site.

Staff in participating clinics will be provided with a secure login and will be required to action two-factor authentication to be able to enter registry data and view data entered by the participant. Depending on the level of access provided, clinic staff will be able to update participant data to make sure all comorbidities are collected and make required updates if the participant notifies them of a change in name, change in address or other issues. Clinic staff will be able to view registry data reports to assist in treatment decision making.

SECURE DATA HOUSING

REGISTRY HOSTING

The ADR is hosted at BioGrid Australia and is secured through Internet Information Services (IIS) for Windows Server which is hosted on the BioGrid DMZ server providing Secure Socket Layer (SSL) communications. The registry database server containing participant data is stored separately from the web application server for added security. Nominated BioGrid staff who maintain the registry will have access to all registry data for the purposes of database maintenance and registry reporting.

The registry data are stored on dedicated BioGrid servers within the Melbourne Health IT environment as part of the service agreement between BioGrid and Melbourne Health.

SERVER BACKUPS AND SECURITY

The BioGrid servers within the Melbourne Health IT environment are backed up daily with protocols in place to restore and recover the registry data if for any reason the registry data are lost or damaged by a power outage, cyberattack, disaster, human error or any other unforeseen even. Each month security patching is applied to BioGrid servers and applications to ensure registry security is kept up to date.
Please refer to BioGrid's Technology and Data Security Charter for more information (link)

DATA CUSTODIAN

The storage, security and management of the registry data is the responsibility of the ADR Data Custodian. The ADR Data Custodian must ensure that data collected within the registry complies with the legal, ethical and best practice guidelines to protect the privacy and confidentiality of the registry participants and participating sites.

SECURE DATA ACCESS – SAS PLATFORM

BioGrid utilises SAS Enterprise Guide and SAS Visual Analytics to view and analyse data in a secure environment. The registry data will be linked to the BioGrid SAS platform enabling registry staff to view, extract, and analyse registry data. The linked data are de-identified with identifiers including name, date of birth, and address, removed from the linked dataset. This reduces the risk of identifiable data being accessed or utilised in reporting.

The periodic static reporting from SAS Visual Analytics will be available for all registry staff, users and external supporters to access through the password protected registry. All reporting will be on aggregated de-identified data to protect the participants' and participating sites' privacy. Where the sample size is less than five, the results will not be published as sample sizes this small could potentially be re- identifiable.

ACCESS TO THE REGISTRY

The ADR is a secure password protected online database with access only to authorised users. The registry utilises a two-factor authentication process to login to the registry.

Two-factor authentication (2FA) is a specific type of multi-factor authentication (MFA) that strengthens access security by requiring two methods (also referred to as authentication factors) to verify the users identify. These factors can include username and password, plus a smartphone app or a registered site IP address to approve authentication requests.

2FA protects against phishing, social engineering and password brute-force attacks and secures logins from attackers exploiting weak or stolen credentials.

REGISTRY USERS

The ADR has established five levels of user access to support data entry, data monitoring and cleaning, and use of the registry data.

A single user may be authorised to have access at multiple sites. Users may also have different levels of access at different sites, e.g. a dermatologist may be a site user for a public clinic but be a site manager for their private rooms.

	Registry Staff	Site Manager	Site User	Research User	External supporters
Access data	All sites	Nominated site	Nominated site	Nominated site	No access
Add data	Yes	Yes	Yes	No	N/A
Modify data	Yes	Yes	Within 24 hours	No	N/A
Delete data	Yes	Yes	No	No	N/A
Add new user	Yes	No (but can nominate a	No	No	No

		new user to registry staff)			
Inactivate user	Yes	Yes	No	No	No
Access registry aggregate summary reports	Yes	Yes	Yes	Yes	Yes

To guarantee the registry data are protected from unauthorised access, only the core registry staff can add a new user to the registry. Any users requiring access to the registry must obtain approval from the sites nominated site manager prior to registry access being granted. The site manager will provide to the registry the user's full name, email address, contact phone number, profession (e.g. dermatologist, registrar, nurse, researcher, etc.) and level of access required to enable the account to be set up.

When a staff member leaves a clinic, the site manager or registry staff can inactive their account, preventing the user from accessing participant data at the site. User access will be regularly reviewed to ensure there is no unauthorised access to registry participant data.

ACCESS TO DATA FOR RESEARCH PURPOSES

Sites contributing participant data to the registry can request access to de-identified data from the registry for research purposes. (See Data Access Policy)

De-identified data for research studies can only be accessed and extracted by registry staff through the BioGrid SAS Enterprise Portal. Access to the BioGrid SAS Enterprise Portal is only to authorised registry staff and nominated BioGrid staff who maintain the system.

Registry data can only be extracted through the BioGrid SAS Enterprise Portal allowing for only authorised projects with appropriate ethics approval to obtain registry data.

Once the de-identified data are extracted, the file will be password protected and transferred directly to the researcher using secure data transfer processes.

ADR SECURITY STANDARDS AND PRINCIPLES

The ADR complies with the following federal and state legislation to protect the privacy of the registry participants. These guidelines are utilised as the basis of the purpose, development, governance, data custodianship and operation of the registry.

National	The Privacy Act 1988, section 95
Australian Capital Territory	The Privacy Act 1988 Health Records (Privacy and Access) Act 1997
New South Wales	Health Records and Information Privacy Act 2002
Northern Territory	Information Act 2002

Queensland	Information Privacy Act 2009 Health and Hospital Network Act 2011 Private Health Facilities Act 1999 Public Health Act 2005
South Australia	Cabinet Administrative Instruction 1/89: Information Privacy Principles 1, 2 & 3; Code of Fair Information Practice
Tasmania	Personal Information Protection Act 2004
Victoria	Health Records Act 2001 Health Services Act 1988 Mental Health Act 1986
Western Australia	Hospital and Health Services Act 1927