StewartBrown
Chartered Accountants

+61 2 9412 3033 info@stewartbrown.com.au
PO Box 5515, Chatswood NSW 2057, Australia
Level 2, Tower 1, 495 Victoria Avenue, Chatswood NSW 2067
www.stewartbrown.com.au

ARC Funding Analysis – Data Security FAQs

General Data Protection Overview

StewartBrown have entered in a non-disclosure agreement (NDA) with the Aged Care Association (ACA) of New Zealand to ensure legal protection of the privacy of member data is in place. In addition to the NDA the following criteria and arrangements apply:

- Data collected will only be used for the purpose of the Aged Residential Care (ARC) Funding Analysis project
- StewartBrown are required to comply with the code of ethics governed by Chartered Accountants Australia and New Zealand. More information here
- Data is stored in a secure database – ARC Funding Analysis portal
- NDA agreements can be entered into with operators who require additional protections over the use of their data. It would be up to each individual operator to prepare the NDA and meet their legal costs for preparing the NDA. Our experience is this is only requested by Listed Entities who have higher security thresholds due regulations in place to minimise risks of market manipulation and they have in-house legal teams who can prepare the agreements

StewartBrown have a trusted reputation with providers across the Australian Aged Care Sector for delivering independent and reliable financial benchmarking services. Established over 30 years ago, this specialist service now regularly supports the needs of 50% of the Australian residential aged care sector, equating to approximately 1,300 homes on a quarterly basis.

Our firm is also trusted by the Australian Government and Independent Health and Aged Care Pricing Authority with regular engagements involving analysing confidential government datasets across numerous consultancy engagements in the Aged Care Sector.

How is provider data transferred to StewartBrown?

There are two methods available.

1. Email data collection templates to ACANZ.fundinganalysis@stewartbrown.com.au
2. For Providers who require a more secure data transfer methods, the standard method used for such file transfer is Microsoft Teams/SharePoint.

Note the sensitivity of the data being collected is financial data aggregated at the corporate/business unit level. The data collected does not include sensitive personal data relating to individual residents, families and employee records.

Many organisations including listed entities and charitable organisations are required to publicly report their financial results as part of their annual compliance. Therefore, due to the nature of the aggregated financial data collected, over 90% of participants are comfortable submitting their data collection via email.

For participants requiring more secure data transfer arrangements please contact ACANZ.fundinganalysis@stewartbrown.com.au to request a data room to be setup.

Will StewartBrown share our data with the ACA?

Data and analysis shared with the ACA is aggregated data where no individual home or operator is identifiable. StewartBrown treat all ARC Participant data in strict confidence and will not share your data with the ACA.

The only way the ACA will have access to your data is if you choose to directly share your data with the ACA. There are situations where you may choose to share your data with the ACA, for example you may request the ACA Data Insight Specialist to help you review your allocation methodologies.

If you do not wish the ACA to have access to your data but require advice on allocation methodologies, then you can work directly with the StewartBrown Team who are independent of the ACA.

Will StewartBrown share our data with the Government and other Stakeholders?

The ARC Funding Analysis is independent of Government. The data reported to Government agencies by the ACA to lobby for financially sustainable and investible aged residential care sector is at an aggregated and de-identifiable level. Government will not have data at individual facility or operator level. This data is held securely in the StewartBrown ARC Funding Analysis portal.

Can Government, journalist and other Stakeholders use the Official Information Act to obtain our data?

No. The ARC Funding Analysis is independent of Government, therefore a journalist cannot obtain your data via the Official Information Act (OIA) process. The only data that government will have is the de-identifiable aggregated analysis that will be made publicly available in the final report to lobby key stakeholders for financially sustainable and investible funding reforms.

Will StewartBrown share our data with other ARC Participants?

No. ARC Participants will not be able to access individual competitor data and likewise other ARC Participants will not be able to access your data. Benchmark reporting will be made available to ARC Participants, but this benchmark data will be aggregated with minimum size datasets that do not enable identification of any single aged residential care home or operator

Where is data stored?

ARC Funding Analysis data is uploaded directly into a secure SQL database structure located in Microsoft Azure Data Centre's (Australia East).

What Security Certificates are held by StewartBrown?

Our Benchmarking Survey portal uses SSL Certificates (PKCS #1SHA-256 With RSA Encryption). These are valid until February 2027 and will be renewed on that date.

What other security controls are in place to protect data assets?

1. Microsoft Teams uses AES-256 encryption for data at rest and in transit
2. All StewartBrown devices have BitLocker encryption enabled and have 15-minute locks after inactivity

3. StewartBrown has the following IT policies which staff must read and accept as part of their onboarding process:
    - StewartBrown IT Policies Combined (Acceptable use policy and others)
    - StewartBrown Cyber Security Policy
    - StewartBrown Data Breach Response Plan (V1.3)
    - StewartBrown External File Sharing Policy
    - StewartBrown AI Policy
4. All StewartBrown staff require multifactor authentication (MFA) on their user accounts. Administrator accounts have Phish-resistant MFA enabled
5. All StewartBrown staff are required to change their password every 90 days
6. Benchmark Survey administrators are required to use two-factor authentication (2FA) to access the website
7. All StewartBrown user devices are set to automatically receive and install Windows Updates
8. All StewartBrown user devices are set to automatically receive updates and patches for installed software once a week
9. StewartBrown staff receive alerts regarding software/hardware vulnerabilities through Microsoft Defender. Alerts are investigated, evaluated and addressed in a timely manner if required
10. All server infrastructure (web server and SQL database server) is hosted in Microsoft Azure. Operating on modern supported operating systems and Microsoft Defender for Cloud Servers. Access to these servers is only available to StewartBrown IT staff via administrator credentials
11. The StewartBrown ARC Funding Analysis portal has been coded to prevent any OWASP vulnerabilities (e.g. SQL injection attacks)
12. Providers can set all provider user accounts (opt-in) with access to provider ARC Funding Analysis data to have 2FA (email)