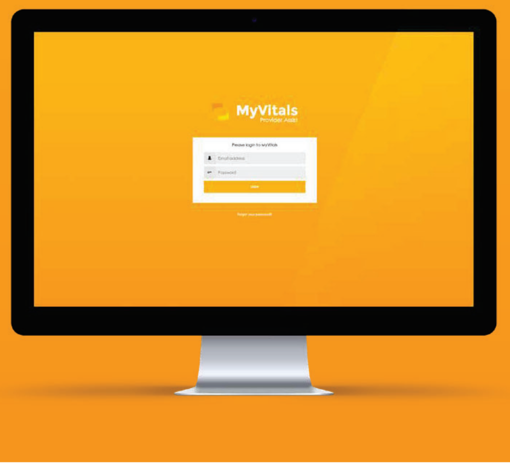
SECURE DATA FACT SHEET

Provider Assist

Provider Assist take Privacy, Data and Cyber Security very seriously. The new Aged Care Legislation Amendment (Single Quality Framework) Principles 2018, due to come into effect as of 1st July 2019, means there is an additional focus on ensuring the privacy of all Residents. It is crucial that personal information is always protected and Providers implement measures to guarantee security. You can keep a copy of this document and Provider Assist's technical overview on file for future reference.

Provider Assist team members are governed by

- **The Privacy Act 1988** (Cth)
- **Our Privacy Policy** *https://providerassist.com.au/privacy-policy/*
- **Relevant IT policies**
- **Password Change and Management Policy** including 2-factor authentication
- **The Privacy Ammenment (Notifiable Data Breaches) Act 2017, and Provider Assist's own Notifiable Data Breach Police and associated response**



SECURE DATA FACT SHEET

Provider Assist

If I use the MyVitals portal, it means my Resident data is with Provider Assist. How do I know my data is safe?

Provider Assist have multiple systems in place to ensure the privacy and security of all data:

1. Provider Assist complies with the Privacy Act 1988 (Cth) when providing all Services. Our Privacy Policy can be found https://providerassist.com.au/privacy-policy/
2. Provider Assist (PA) Data Breach Response Plan is to set out procedures and lines of authority for PA in the event that PA experiences a data breach (or suspects that a data breach has occurred). This Plan is intended to enable PA to contain, assess and respond to data breaches in a timely fashion and to mitigate potential harm to affected individuals. You can read our Notifiable Data breach guidelines here: https://providerassist.com.au/notifiable-data-breach/
3. PA are secured by the Bitlocker Remote wipe. If a computer is suspected to have been compromised it can be wiped remotely immediately.
4. Quarterly Security Check: To ensure the security of your organisation's data, it is important to delete users regularly who are no longer working with your organisation. Your MyVitals Administrator at your organisation will be responsible for this. However, we will send a Reminder email each quarter to MyVitals Administrators to clear out old users!

IMPORTANT TO NOTE: Cyber security starts with you. The biggest risk to a system are weak passwords and not deleting former users. Keep your Passwords long and strong and reguarly audit your users and clear out any former team members.

Where is MyVitals data stored?

Data is stored in Sydney, NSW at the Amazon s3 Sydney Data Centre. Data sent from Amazon S3 to MyVitals is encrypted, but also transmitted using a Virtual Private Connection - meaning data never hits a public network. The Amazon S3 instance has monitoring for security breaches.

For information on **AWS data centres** please visit: https://aws.amazon.com/compliance/data-center/data-centers/

For information on **AWS data centre controls** please visit: https://aws.amazon.com/compliance/data-center/controls/

All MyVitals data is deidentified when it is shared for benchmarking.