ADFHSC - Service Provider (SP) Data Sovereignty FAQs

What is data sovereignty?

Data sovereignty means that data must be stored and managed according to the requirements set out in Bupa's contract with the Commonwealth of Australia (CoA). For Bupa, this includes keeping sensitive information such as health records within Australian borders and handling it in line with government expectations around data security, access, and control. As a Service Provider, the main requirement is, any Personal Information or Commonwealth (Defence) Data inclusive of identifiable and de-identifiable records should **not** be transferred, hosted, or accessed from overseas under any circumstances. This includes ensuring no persons outside Australia has **access to, can use** or **disclose** any such information without the written consent of the Department of Defence.

Why is data sovereignty important?

Data sovereignty is important because it helps keep Eligible Personnel (EP) sensitive information safe and under Australian control. If data is stored or accessed outside Australia, it may be exposed to foreign laws, increasing the risk of unauthorised access, hacking or misuse. For Defence work, keeping data in Australia helps protect national security and ensures providers follow data sovereignty requirements.

What is Commonwealth Data?

Includes all data and information relating to the Commonwealth, and its operations, facilities, customers, employees, officers, agents, permitted subcontractors, assets and programs (including Personal Information and Health Information) in whatever form that information may exist and whether entered into, stored in, generated by or processed through software or equipment by or on behalf of the Department of Defence.

For the avoidance of doubt, Commonwealth Data includes (but not limited to):

- EP full names
- Dates of Birth
- Defence Military Ranks
- Locations of services provided to EP who have accessed services via the Defence Bupa Contract
- Australian Defence Force (ADF) email addresses (these typically end in .gov)
- EP Identification number
- Defence Approval Numbers
- Medically Sensitive Information e.g. the referral, clinical reports and/or other
- EP data includes identifiable and de-identifiable records

How do I know if the systems/software I am currently using or plan to use is compliant?

You should confirm that your system stores and processes EP data in Australia and no person outside Australian can access data. Each platform can differ; therefore you should check compliance of your software with your provider or software vendor. It is good practice to have evidence from the vendor in case you are audited. Before contacting the vendor, it can be worth checking the vendor's website and publicly available information for how their information is transferred, transmitted, stored or disclosed.

Contacting the vendor:

1. Send email to IT support
    - *Subject line:* 'Data Residency Request for Evidence'

- *Body of text:* 'Could you please confirm whether [*application, service, software tool*] data (including backups) is stored only in Australia? Please provide screenshots and/or documentation as evidence.'

2. In a reply, you are looking for 'evidence' such as official documentation stating Australian data residency (SLA, Terms of Service, Privacy Policy, contract, vendor statement from website, etc).

For example:



Key Points – Data Residency and Security for Australian Customers

- **All data for Australian accounts is stored in Australia**

  We use Amazon Web Services (AWS) data centres located within Australia to store and back up all customer data for Australian-based Zanda accounts. Data is encrypted both at rest and in transit.

What to do if software vendor/IT indicate data Residency is overseas?
Request EP data is removed from the system that is overseas, or codes are used instead of identifiable EP data that map back to identifiable stored on a separate system hosted in Australia.

Can I utilise people from overseas to perform my clinical and general administration?
No, as no person/s outside of Australia can have access to, use or disclose any EP related information. For the avoidance of doubt, this includes (but is not limited to) medical transcribers, IT support staff, and any staff that are on overseas holidays.

Can I continue to access EP data to work if I am on an overseas holiday?
No, as no person/s outside of Australia can have access to, use or disclose any EP related information, even in unique or urgent circumstances

Can I continue to work with EPs via telehealth if I am relocating overseas?
No, the EP cannot be treated while you are offshore as it would mean their information is being transmitted outside of Australia.

What software can I use to deliver Telehealth Services (phone calls and video conferencing)?
Consultations carried out via Telehealth must be conducted via Coviu or a platform which meets or exceeds the required privacy, security and data sovereignty standards.

Can I continue to use my current software for non-Defence members?
Yes, the data sovereignty obligations from Defence in relation to information transferred, transmitted, stored or disclosed (including in Cloud computing arrangements) outside of Australian Territories only applies to Commonwealth Data. Therefore, any systems utilised relating to non-Defence clients can continue as per usual requirements.

What do I do if I receive the data sovereignty Audit Questionnaire for an Audit by Bupa ADF?
Please have someone familiar with your data security practices, complete the form to the best of your ability and consult your internal experts if needed.

How do I ensure my practice stays compliant with the Commonwealth of Australia's (Defence) Data sovereignty obligations?

- Data sovereignty applies to all people who engage in any matter relating to an EP including (but not limited to) anaesthetists, assistant surgeons, nurses, practice managers and reception staff etc.
- Always follow privacy standards when collecting or sharing patient information.
- Ensure your practice has clear protocols and processes in place to support data Sovereignty compliance as per Defence in relation to EPs. This can include documented work instructions for staff, regular training on data safety, and confirmation of compliance status from vendors whose systems are used. These measures help ensure data is handled appropriately and in line with ADF requirements.
- Service Providers should only give staff access to the data they need for their role and use individual and strong passwords along with Multi-Factor Authentication (MFA) to protect your systems. Best practice is to ensure all of your staff are using MFA to access all the software used by your practice.

Where can I keep up with important systems updates/impacts?

Any updates can be found at the https://www.bupa.com.au/campaigns/adf-hsc-provider-hub alongside email communications from Bupa ADF for any changes.

I would like to speak to someone on this further, who can I contact?

Please contact the Assurance team via email at ADFassurance@bupa.com.au for any questions relating to Commonwealth Data sovereignty requirements.