SOLUTION ARCHITECTURE FACTSHEET

Is the solution that supports UTAS single or multi tenanted?
Multi-Tenanted

Are the Databases that support the solution shared?
Yes

If the Database that contains UTAS data is shared with other customers how is the integrity of the data guaranteed?
We have segregation at Infrastructure and logical level in Microsoft Azure. C2C has strict security management processes and protocols to ensure customer data is handled to adhere to compliance.

If the DataBase that contains UTAS data is shared how is the DataBase Schema structured to manage Client Data securely?
Clinic to Cloud technical architecture logically segregates and protect individual clients. Every practice has a unique identifier and gets validated in multiple layers (e.g database, services and UI).

Is the data encrypted at rest?
Clinic to Cloud encrypts data both in transit and at rest. We utilise AES-256 encryption on the SQL database and Data Storage at rest and TLS 1.2 during transit.

Are you required to store UTAS data for a defined retention period?
Yes, it is 7 years (the medical legislation requires that medical records should be kept until such time as there is little or no risk of litigation arising from the patient's treatment).

What is the data retention period?
PITR 35 days, frequency is 10 minutes. Weekly LTR Backups: 1 year. Monthly LTR Backups: 7 years. Yearly LTR Backups: keeping the week 1 for 7 years.

In what format/s is the data managed in for the retention period?
SQL backups

Which endpoint protection is used on the servers that support the solution?
Azure Security Centre & Windows Defender ATP