Security Overview

How Siace Partners accesses, processes, stores, and protects your dental practice data.

WHAT WE ACCESS

Financial data via Xero - transaction records, invoices, payroll data, BAS information, and bank feeds. Access is established through OAuth 2.0. We never see or store your Xero password. You can revoke access at any time from within your Xero account.

Operational data via your practice management system - appointment records, schedule data, provider productivity, and revenue metrics. Accessed via read-only database accounts with permissions scoped to the specific tables required.

What we never access: clinical records, medical histories, clinical notes, or imaging. Patient health information never enters our platform.

WHERE YOUR DATA LIVES

Hosting	Detail
Cloud provider	Microsoft Azure, Australia East region (Sydney)
Data residency	All data stored in Australia. No data leaves Australian jurisdiction.
Encryption at rest	AES-256 via Azure Storage Service Encryption
Encryption in transit	TLS 1.2 minimum on all connections
Secrets management	Azure Key Vault. No credentials in application code.
Azure certifications	ISO 27001, SOC 2 Type II, IRAP (Australian govt/healthcare)

HOW WE PROTECT YOUR DATA

Read-only access: We look, we never modify. Your Xero and PMS remain your systems. We extract data for analysis only.

Clinic isolation: Every record is tagged with a clinic identifier. Row-level security enforced at the database layer. One practice's data can never be seen by or mixed with another.

Access control: Azure Entra ID with role-based access and mandatory multi-factor authentication. Every access event logged. Quarterly access reviews.

Human approval on financials: AI assists with analysis and pattern detection. AI does not have authority to move money, post journals, lodge BAS, or take any action with financial consequence without human review.

Credential security: OAuth 2.0 for Xero (we never see your password). Dedicated read-only service accounts for PMS. All secrets managed in Azure Key Vault.

Breach notification: If a data breach affects your data, we notify you within 72 hours under the Notifiable Data Breaches (NDB) scheme of the Australian Privacy Act.

COMPLIANCE FRAMEWORK

We operate under the **Australian Privacy Act 1988** and the **13 Australian Privacy Principles (APPs)**. We comply with the **Notifiable Data Breaches (NDB) scheme**.

For practices in Singapore, we also comply with the **Personal Data Protection Act 2012 (PDPA)**.

YOUR RIGHTS

Right	Detail
Revoke access	Disconnect Xero OAuth at any time from within your Xero account. Request PMS access removal.
Data deletion	On termination, we delete your data within 90 days unless legally required to retain.
Access your data	Request a copy of personal information we hold. We respond within 30 days.
No lock-in	30 days written notice to terminate. No exit fee. No data extraction charge.
Complaint	Contact hello@siacepartners.com or escalate to the OAIC (oaic.gov.au).

AZURE DEPLOYMENT POLICY

The following controls are enforced at the Azure infrastructure level to ensure the claims in this document are technically provable and auditable.

#	Control	Implementation
1	**Region restriction**	Azure Policy assigned at subscription level restricts all resource creation to Australia East and Australia Southeast regions only. Any attempt to deploy outside these regions is denied.
2	**TLS enforcement**	Minimum TLS version set to 1.2 on all Storage Accounts, Azure SQL databases, and App Services. Verified via Azure Policy compliance audit.
3	**Secrets in Key Vault**	All application secrets, connection strings, and API keys stored in Azure Key Vault. Application code references Key Vault URIs only. No secrets in environment variables, config files, or source control.
4	**Azure OpenAI region**	Azure OpenAI Service deployed in Australia East region. Model deployment confirmed to Australian data centre. No data processed outside Australian jurisdiction.
5	**Diagnostic logging**	Diagnostic settings enabled on Key Vault, Storage Accounts, and Azure SQL. Logs shipped to immutable storage with 12-month retention. Supports audit and incident investigation.
6	**Encryption defaults**	Azure Storage Service Encryption (AES-256) and Azure SQL Transparent Data Encryption (TDE) confirmed active on all resources. These are enabled by default and cannot be disabled.
7	**Access review cadence**	Quarterly review of all Azure Entra ID role assignments and Key Vault access policies. Stale or excessive permissions removed. Review log retained.

These controls are configured before any client data is onboarded. Compliance status is verifiable through Azure Policy dashboards and diagnostic logs at any time.

Questions? Contact us at hello@siacepartners.com or visit siacepartners.com/data-security for full details.