Software Requirements Specification (SRS)

System: Patient Record Summarisation
Compliance: Australian Dental Standards, Privacy Act 1988, Dental Board of Australia

---

1. Introduction

1.1 Purpose

The purpose of the "Patient Record Summary" workflow is to securely process patients' records, appointment notes, dentist notes, and scan summaries, and generate a concise history summary. This supports dentists in delivering safe, evidence-based, and timely dental care in compliance with Australian Dental Board standards.

1.2 Scope

The workflow integrates with the secure patient database, extracts relevant records, and applies a summarisation process. The system ensures that data is handled in compliance with the **Australian Privacy Principles (APPs)** and the **Dental Board of Australia's requirements for clinical record-keeping**. Summaries assist dental practitioners in clinical decision-making and continuity of care.

---

2. Overall Description

2.1 System Overview

- *Connects to the authorised patient record database.*
- *Retrieves appointment history, clinical notes, and diagnostic scan summaries.*
- *Generates a structured clinical history while ensuring accuracy and completeness as required by **ACSQHC clinical safety standards**.*

2.2 Users and Use Case

- ***Primary Users:** Registered Dentists and Dental Specialists.*
- ***Secondary Users:** Authorised dental support staff (with role-based access).*
- ***Use Case:** A dentist requests a compliant patient summary prior to or during a consultation. The workflow generates a history summary for safe and efficient care delivery.*

---

3. System Requirements

3.1 Functional Requirements

- *Securely connect to the **Supabase patient record database**.*
- *Retrieve patient records, appointment notes, and dentist notes.*
- *Employ a **Summarisation Agent** to create an accurate, unbiased, and traceable history summary.*
- *Use the **MCP Tool** for controlled workflow execution.*
- *Output summary must comply with **Dental Board of Australia's record-keeping requirements** (accuracy, completeness, authorship, date).*

3.2 Non-Functional Requirements

- ***Performance:** Summaries must be generated within 5 seconds per patient record.*
- ***Privacy & Security:***
    - *Encrypt data in transit and at rest.*
    - *Restrict access with role-based authentication.*
    - *Comply with **Privacy Act 1988 (Cth)** and **Australian Privacy Principles (APPs)**.*
- ***Record-Keeping Standards:** Align with **Dental Board of Australia's Guidelines for Dental Records**, including retention and auditability.*
- ***Auditability:** Each summary generated must be logged with timestamp and practitioner ID.*

---

4. External Interfaces

- ***Database:** Supabase (patient records, appointment history, dentist notes).*
- ***Summarisation Agent:** AI-driven clinical summarisation tool.*
- ***MCP Tool:** Workflow execution and integration, ensuring compliance with audit and security logging.*

---

5. Compliance References

- **Dental Board of Australia – Guidelines for Dental Records**
- **Australian Commission on Safety and Quality in Health Care (ACSQHC) Standards**

- **Privacy Act 1988 (Cth) – Australian Privacy Principles (APPs)**
- **Code of Conduct for Registered Health Practitioners (AHPRA)**
- **Health Records and Information Privacy Act 2002 (NSW)** and equivalent state/territory health records laws

---

6. Risk Management

6.1 Identified Risks and Mitigations

Risk	***Impact***	***Mitigation Strategy***
Data Breach or Unauthorised Access	*Compromise of sensitive patient information, legal non-compliance under Privacy Act 1988*	*Enforce encryption, role-based access, regular penetration testing, audit logging*
Incorrect or Incomplete Summarisation	*Misleading patient history may result in poor clinical decision-making*	*Implement validation workflows, allow dentist review/override, maintain traceability to original records*
System Downtime	*Inability to access patient summaries during clinical care*	*Ensure high availability architecture, implement failover and backup systems*
Regulatory Non-Compliance	*Legal penalties, loss of accreditation, reputational damage*	*Align workflows with Dental Board guidelines, ACSQHC standards, and regular compliance audits*
Data Retention or Deletion Errors	*Breach of record-keeping obligations under Australian dental standards*	*Implement automated retention schedules, compliance checks, and audit trails*
User Misuse (Improper Access or Export)	*Breach of confidentiality or improper record handling*	*Enforce user training, strict permissions, monitoring of access logs*

6.2 Risk Governance

- *Risk assessments conducted annually in line with **Dental Board of Australia** and **ACSQHC safety standards**.*

- *Incident response procedures follow **Australian Privacy Principle 11 (APP 11)** obligations.*
- *Audit logs reviewed quarterly by the compliance officer.*

---

7. Data Retention & Disposal Policy

7.1 Retention Requirements

- ***Minimum Period:** Patient records and summaries must be retained for at least **7 years after the last patient contact**, in line with the **Dental Board of Australia's Guidelines for Dental Records**.*
- ***For Minors:** Records must be retained until the patient reaches **25 years of age**, or for 7 years after the last entry — whichever is longer.*
- ***Legal Compliance:** Retention aligns with the **Health Records and Information Privacy Act 2002 (NSW)** and equivalent state/territory legislation.*

7.2 Disposal Policy

- ***Secure Disposal:** At the end of the retention period, records and summaries must be securely destroyed using approved methods (e.g., secure digital erasure for electronic files, cross-shredding for paper records).*
- ***Audit & Verification:** Disposal must be logged and verified by the compliance officer, with signed records of deletion maintained for accountability.*
- ***Prohibition on Unauthorised Deletion:** Users cannot delete or modify records outside of policy. Access is restricted to compliance staff for authorised record disposal.*

7.3 Backup & Recovery

- *Regular encrypted backups must be maintained and stored securely in Australia, ensuring recovery in case of system failure.*
- *Backup retention must follow the same timeframes as primary records, with disposal policies applied consistently.*

---

8. Compliance Matrix

Requirement	Relevant Standard / Law	Reference
Patient data must be encrypted in transit and at rest	Privacy Act 1988 (Cth), APP 11 – Security of personal information	APP 11
Access must be restricted to authorised users via role-based controls	Privacy Act 1988 (Cth), Dental Board Guidelines – confidentiality	APP 6, Dental Records 2.1
Summaries must be accurate, complete, and traceable to original entries	Dental Board of Australia – Guidelines for Dental Records	Section 3.2 & 3.4
Each summary must log author, date, and timestamp	Dental Board of Australia – Record keeping requirements	Section 4.2
Retain patient records for at least 7 years after last entry	Dental Board of Australia – Guidelines for Dental Records	Section 3.8
Retain minors' records until age 25 or 7 years after last entry (whichever longer)	Dental Board of Australia – Guidelines for Dental Records	Section 3.8
Secure destruction of records after expiry of retention period	Health Records and Information Privacy Act 2002 (NSW), Privacy Act 1988	HPP 4, APP 11
Backup and disaster recovery for continuity of care	ACSQHC National Safety and Quality Health Service Standards (NSQHS), Standard 1 – Clinical Governance	NSQHS 1.10
Summaries generated within 5 seconds	ACSQHC – Clinical safety and performance efficiency	NSQHS 1.27
Incident response plan for data breaches	Privacy Act 1988 (Cth), Notifiable Data Breaches Scheme	APP 11, NDB Scheme
Risk assessments conducted annually	ACSQHC – Continuous improvement and safety	NSQHS 1.09