SPECIALIST PRACTICE QUALITY FRAMEWORK

# Domain 5: Information Governance and Health Records

We manage patient information securely and in accordance with our legal obligations.

Version 1.0 — First Edition

Published by the SPQF Editorial Group

# Why This Domain Matters

Every specialist practice holds thousands of clinical records, many containing some of the most sensitive information a person will ever generate - psychiatric histories, sexual health diagnoses, genetic test results, fertility treatment records, cancer staging. A breach is not just a compliance problem. It is a deeply personal violation for the patients affected and an existential reputational event for the practice.

Yet information governance in specialist practices is often remarkably informal. Records sit in clinical software that nobody has audited for access permissions. The practice manager's personal email is used to send referral letters. Backups run to a hard drive under the reception desk that nobody has tested in two years. Passwords are shared. Former staff still have login credentials. The My Health Records system is enabled but nobody is checking what gets uploaded.

The regulatory environment is tightening. The Notifiable Data Breaches scheme means that a breach involving health information almost always requires notification to the OAIC and affected individuals. The Privacy Act review is flagging healthcare as a priority sector. And cyber attacks on Australian healthcare providers are no longer rare - they are routine.

This domain helps practices move from informal habits to documented, defensible information governance. Most of the indicators are not technically difficult. They just require someone to actually do them.

# Quality Statements

## 5.1 — Clinical Record Quality

*Our clinical records are accurate, complete, and support the safe continuity of care.*

**INDICATORS**

**5.1.1** The practice uses a clinical record system - whether electronic or paper - that allows each patient encounter to be documented in a structured, legible, and retrievable way. Electronic health records are strongly preferred and used as the primary record in the vast majority of specialist practices.

**5.1.2** Clinical records include, at a minimum, the patient's demographic details, relevant medical history, current medications and allergies, the presenting issue, clinical findings, diagnosis or differential diagnosis, management plan, and any referrals or investigations ordered.

**5.1.3** Every clinical entry is attributable to the clinician who made it and is dated. In electronic systems, audit trails are enabled and preserved. In paper records, entries are signed and dated.

**5.1.4** Records are updated contemporaneously - during or immediately after the consultation. Retrospective amendments are clearly identified as such, dated, and attributed. Original entries are not deleted or overwritten.

**5.1.5** The practice has a process for reconciling clinical information received from external sources - referral letters, hospital discharge summaries, investigation results, correspondence from other providers - into the patient's record.

**5.1.6** The practice periodically audits a sample of clinical records for completeness and quality. Audit findings are shared with clinicians and used to improve documentation standards.

SUGGESTED EVIDENCE

- Description of clinical record system and structure
- Record-keeping policy or standard
- Examples of completed clinical records (de-identified)
- Audit trail configuration in electronic system
- Clinical record audit reports and resulting actions

## 5.2 — Privacy and the Australian Privacy Principles

*We comply with the Privacy Act 1988 and the Australian Privacy Principles in how we collect, use, store, and disclose patient information.*

INDICATORS

**5.2.1** The practice has a current privacy policy that describes how it collects, holds, uses, and discloses personal and health information. The policy is available to patients - on the practice website, in reception, or provided at intake.

**5.2.2** Patients are informed at or before their first consultation about why information is being collected, how it will be used, who it may be shared with (e.g., referring GP, other treating practitioners, Medicare, private health insurers), and their rights of access and correction.

**5.2.3** Personal and health information is collected only for purposes that are directly related to the practice's functions. The practice does not collect information that is not reasonably necessary for the provision of care or the administration of the practice.

**5.2.4** The practice only discloses patient information with the patient's consent, or where disclosure is authorised or required by law (e.g., mandatory notifications, subpoenas, public health reporting). Staff understand the difference between these categories and know when to seek guidance.

**5.2.5** The practice has a process for responding to patient requests for access to their health records, consistent with APP 12. Requests are actioned within 30 days. Where access is refused (which is rare and must be justified), the reason is documented and the patient is informed of their right to complain to the OAIC.

**5.2.6** The practice has a process for correcting clinical records when a patient identifies an error, consistent with APP 13. Corrections are made as amendments - original entries are not deleted.

SUGGESTED EVIDENCE

- Privacy policy (patient-facing)
- Privacy collection notice or intake form privacy statement
- Process for handling access requests with timeframe tracking
- Process for handling correction requests
- Staff training records on privacy obligations

## 5.3 — Data Security

*We protect patient information from unauthorised access, loss, misuse, and interference.*

**INDICATORS**

**5.3.1** Access to clinical records is restricted to authorised personnel on a need-to-know basis. User accounts are individual - shared logins are not used. Access levels are appropriate to each person's role (e.g., reception staff do not have the same clinical record access as treating clinicians).

**5.3.2** Passwords are unique, sufficiently complex, and changed in accordance with the practice's policy. Multi-factor authentication is enabled for clinical systems and remote access where the system supports it.

**5.3.3** When a staff member leaves the practice or changes role, their system access is reviewed and revoked or adjusted on the day of departure or role change. The practice maintains a record of active user accounts and reviews it at least annually.

**5.3.4** Workstations and devices that access clinical records are physically secured and configured to lock automatically after a period of inactivity. Mobile devices used to access patient information are encrypted and protected by passcode or biometric authentication.

**5.3.5** The practice's network is protected by current firewall, antivirus, and anti-malware software. Operating systems and clinical software are kept up to date with security patches. The practice has a nominated person or external provider responsible for IT security.

**5.3.6** Paper records, where they still exist, are stored securely with access limited to authorised staff. Records in transit (e.g., being transported between rooms or to off-site storage) are managed to prevent loss or unauthorised access.

**5.3.7** The practice has considered the security of its clinical software vendor, including where patient data is hosted, whether data is encrypted at rest and in transit, and what the vendor's obligations are in the event of a breach. This is documented or addressed in the vendor agreement.

**SUGGESTED EVIDENCE**

- User access register and role-based access configuration
- Evidence of individual logins (no shared accounts)
- Offboarding checklist including access revocation
- IT security measures documentation
- Vendor security assessment or contract clauses
- Physical security measures for paper records

## 5.4 — Backup and Disaster Recovery

*We can recover our clinical records and resume operations if our systems fail.*

**INDICATORS**

**5.4.1** The practice performs regular automated backups of its clinical records and critical business data. Backups occur at least daily. For practices using cloud-hosted clinical software, the vendor's backup arrangements are understood and documented.

**5.4.2** Backups are stored in a location that is separate from the primary system - either off-site, in the cloud, or on media that is physically removed from the premises. Backups are encrypted.

**5.4.3** Backup restoration is tested at least annually. The practice has confirmed that it can actually recover data from its backups - not just that backups are running. The test is documented.

**5.4.4** The practice has a business continuity plan that addresses how it will operate if its clinical system becomes unavailable - whether due to a technical failure, ransomware attack, natural disaster, or vendor outage. The plan includes how patients will be seen, how critical information will be accessed, and who is responsible for activating the plan.

**5.4.5** The practice has considered how long it can operate without its clinical system (recovery time objective) and how much data it can afford to lose (recovery point objective). These are realistic assessments, not aspirational statements.

SUGGESTED EVIDENCE

- Backup schedule and configuration
- Backup storage location and encryption details
- Backup restoration test records
- Business continuity plan
- Vendor backup and SLA documentation

## 5.5 — Secure Communication

*We transmit patient information securely and appropriately.*

INDICATORS

**5.5.1** The practice uses secure electronic messaging for the transmission of clinical correspondence - referral letters, reports, investigation requests. Secure messaging platforms (e.g., Medical Objects, Argus, HealthLink, or equivalent) are preferred over standard email for routine clinical communication.

**5.5.2** Where standard email is used for communication that contains patient-identifiable information, the practice has assessed the risk and applied appropriate safeguards - such as encryption, password-protected attachments, or confirmation of the recipient's email address. Staff understand that unencrypted email is not a secure channel for health information.

**5.5.3** Fax, where still used, is treated as an insecure channel. The practice has assessed whether fax can be replaced and, if it remains in use, has safeguards to prevent misdirected faxes (e.g., confirming the number, using programmed speed dials, verifying receipt).

**5.5.4** Patient communication via SMS, patient portals, or messaging apps is governed by a policy that addresses what information can and cannot be communicated through each channel, and whether the patient has consented to that channel being used.

**5.5.5** The practice has a process for verifying the identity of a person requesting patient information by phone, particularly where the request comes from someone claiming to be the patient, a family member, or another health provider.

SUGGESTED EVIDENCE

- Secure messaging system documentation
- Email and fax usage policy for clinical information
- Patient communication channel policy
- Identity verification process for phone requests
- Staff training records on secure communication

## 5.6 — My Health Record

*We understand our obligations under the My Health Records system and manage our participation appropriately.*

**INDICATORS**

**5.6.1** The practice is registered as a participating healthcare provider organisation in the My Health Record system (or has made a documented decision about its participation status and understands the implications).

**5.6.2** Staff who access the My Health Record system understand their obligations under the My Health Records Act 2012, including the permitted purposes for access, the prohibition on unauthorised access, and the penalties for misuse.

**5.6.3** The practice has configured its clinical software to upload relevant documents to patients' My Health Records (e.g., specialist letters, event summaries, discharge summaries) where the patient has a My Health Record and has not restricted access.

**5.6.4** The practice checks a patient's My Health Record where doing so would support safe clinical care - for example, to review shared health summaries, medication lists, or allergy information, particularly at the first consultation or when prescribing.

**5.6.5** The practice has a process for managing situations where a patient requests that information not be uploaded to their My Health Record, or where the practice identifies that incorrect information has been uploaded.

**SUGGESTED EVIDENCE**

- My Health Record registration status
- Staff training records on My Health Record obligations
- Clinical software configuration for My Health Record uploads
- Process for managing patient requests regarding My Health Record

## 5.7 — Record Retention and Disposal

*We retain clinical records for the required periods and dispose of them securely.*

**INDICATORS**

**5.7.1** The practice understands and complies with the applicable record retention requirements. In most Australian jurisdictions, health records for adults must be retained for at least seven years from the date of last entry. For minors, records must be retained until the patient turns 25 (or seven years from the last entry, whichever is later). Longer retention periods apply in some jurisdictions and for specific record types.

**5.7.2** The practice has a documented retention schedule that specifies how long different record types are retained and references the applicable legislation or guideline.

**5.7.3** When records reach the end of their retention period, they are disposed of securely. Paper records are shredded or destroyed by a certified document destruction service. Electronic records are permanently deleted in a manner that prevents recovery. Disposal is documented.

**5.7.4** If the practice closes or a practitioner departs, there is a documented plan for the custody and management of clinical records that ensures ongoing compliance with retention obligations and patient access rights. Patients are given reasonable notice and the opportunity to nominate where their records should be transferred.

**5.7.5** The practice does not dispose of records that are the subject of a current or anticipated complaint, claim, or investigation, regardless of whether the retention period has passed.

**SUGGESTED EVIDENCE**

- Record retention schedule with legislative references
- Secure disposal records or certificates
- Practice closure or practitioner departure record management plan
- Litigation hold process or awareness

# Self-Assessment Summary

| Ref | Indicator |
|---|---|
| 5.1.1 | Structured clinical record system in use |
| 5.1.2 | Records include minimum required content |
| 5.1.3 | Entries attributable, dated, audit trail enabled |
| 5.1.4 | Contemporaneous documentation, no deletions |
| 5.1.5 | External information reconciled into records |
| 5.1.6 | Periodic clinical record audit conducted |
| 5.2.1 | Privacy policy current and available to patients |
| 5.2.2 | Patients informed about information handling |
| 5.2.3 | Collection limited to necessary information |
| 5.2.4 | Disclosure only with consent or legal authority |
| 5.2.5 | Access requests actioned within 30 days |
| 5.2.6 | Correction process without deleting originals |
| 5.3.1 | Role-based access, individual logins, no sharing |
| 5.3.2 | Passwords and MFA appropriately configured |
| 5.3.3 | Access revoked on departure or role change |
| 5.3.4 | Workstations and devices secured |
| 5.3.5 | Network security current and maintained |
| 5.3.6 | Paper records stored securely |
| 5.3.7 | Vendor security assessed and documented |
| 5.4.1 | Daily automated backups running |
| 5.4.2 | Backups stored off-site and encrypted |

| Ref | Indicator |
|---|---|
| 5.4.3 | Backup restoration tested annually |
| 5.4.4 | Business continuity plan in place |
| 5.4.5 | Recovery time and data loss objectives defined |
| 5.5.1 | Secure messaging used for clinical correspondence |
| 5.5.2 | Email safeguards applied for patient information |
| 5.5.3 | Fax risk assessed and safeguards applied |
| 5.5.4 | Patient communication channels governed by policy |
| 5.5.5 | Phone identity verification process in place |
| 5.6.1 | My Health Record registration status confirmed |
| 5.6.2 | Staff trained on My Health Record obligations |
| 5.6.3 | Clinical software configured for MHR uploads |
| 5.6.4 | My Health Record checked for clinical care |
| 5.6.5 | Patient MHR restriction requests managed |
| 5.7.1 | Retention requirements understood and met |
| 5.7.2 | Retention schedule documented |
| 5.7.3 | Secure disposal process with documentation |
| 5.7.4 | Practice closure or departure record plan |
| 5.7.5 | Litigation hold awareness in place |

This document is part of the Specialist Practice Quality Framework (SPQF). Visit spqf.au for the full framework, evidence guides, and self-assessment tools.