SPECIALIST PRACTICE QUALITY FRAMEWORK

Evidence Guide

Domain 5: Information Governance and Health Records

Version 1.0 — First Edition

Published by the SPQF Editorial Group

This guide provides concrete examples of what evidence looks like for each indicator in this domain. Use it alongside your self-assessment to understand what “Established,” “Developing,” and “Excelling” mean in practice.

5.1 — Clinical Record Quality

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

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.

ESTABLISHED EVIDENCE

- Documentation of the clinical record system in use (name, version, hosting arrangement), confirming it supports structured, legible, and retrievable records for each patient encounter
- Evidence that the system is the primary clinical record - not supplemented by informal notes in Word documents, personal notebooks, or unsanctioned apps
- Screen captures or template examples showing the structured fields available for documenting encounters (e.g., history, examination, diagnosis, plan)

MINIMUM FOR DEVELOPING

- An electronic health record is in use for most consultations, but some clinicians still maintain parallel paper notes or use free-text without structured templates

EXCELLING

- The practice periodically reviews whether its clinical software meets current needs, evaluates new features or alternative systems, and has a documented decision log for system-related decisions

COMMON PITFALLS

- The EHR is in use but treated as a billing tool rather than a clinical record - consultation notes are minimal or absent because the clinician "dictates separately" into a system that is not integrated
- Legacy paper records have not been scanned or indexed, making retrieval for returning patients unreliable

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.

ESTABLISHED EVIDENCE

- De-identified examples of completed clinical records demonstrating the required minimum content: patient demographics, relevant medical history, current medications and allergies, presenting issue, clinical findings, diagnosis or differential diagnosis, management plan, and any referrals or investigations ordered
- A documented record-keeping standard or policy that specifies these minimum content requirements for all clinicians
- Evidence that templates or structured fields in the clinical software prompt clinicians to complete each required element

MINIMUM FOR DEVELOPING

- Most records contain the key elements but there is no written standard specifying what must be documented, and completeness varies between clinicians

EXCELLING

- The practice has tailored its record templates to the specialty context (e.g., procedure-specific templates for procedural specialists, standardised mental health assessment fields for psychiatrists) and reviews template adequacy annually

COMMON PITFALLS

- Allergy and medication fields are left blank rather than marked "nil known" - there is no way to distinguish "not asked" from "no allergies"
- Management plans are vague ("continue current management") without specifying what that management is, making handover or locum cover unsafe

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.

ESTABLISHED EVIDENCE

- Demonstration that the clinical software assigns each entry to the logged-in user and timestamps it automatically
- Confirmation that audit trail functionality is enabled and captures who created, viewed, or modified records, with audit logs preserved and not overwritable by standard users
- For any remaining paper records, entries are signed (with legible name), dated, and include the clinician's designation

MINIMUM FOR DEVELOPING

- Entries are attributable and dated in the electronic system, but the audit trail has not been verified as active or has never been reviewed

EXCELLING

- Audit trail reports are reviewed periodically (e.g., quarterly) to identify unusual access patterns, and findings are escalated where appropriate

COMMON PITFALLS

- Clinicians log in under another practitioner's account to "save time" - this destroys attribution and creates medico-legal risk if the record is ever subpoenaed
- Audit trail is technically enabled but nobody knows how to run an audit report, so it has never been checked

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.

ESTABLISHED EVIDENCE

- Policy or documented expectation that clinical entries are made during or immediately after the consultation, not hours or days later
- Evidence that the clinical software prevents deletion of entries and that any amendments are recorded as addenda with the date, time, and author of the amendment clearly visible alongside the original entry
- De-identified example showing how a retrospective amendment appears in the record, demonstrating that the original entry is preserved

MINIMUM FOR DEVELOPING

- Most clinicians document contemporaneously, but there is no written policy and no verification that the system prevents deletions or overwrites

EXCELLING

- The practice monitors documentation timeliness through periodic spot checks and provides feedback to clinicians who routinely document late

COMMON PITFALLS

- Clinicians dictate notes at the end of the day or week, resulting in entries that are inaccurate because details are forgotten - this is a significant medico-legal vulnerability
- The clinical software allows deletion of entries and this capability has not been restricted at the system configuration level

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.

ESTABLISHED EVIDENCE

- A documented workflow describing how incoming clinical information (referral letters, hospital discharge summaries, investigation results, correspondence from other providers) is received, reviewed by the treating clinician, and filed into the correct patient record
- Evidence that the workflow includes a mechanism for the clinician to acknowledge review (e.g., sign-off, electronic acknowledgment) before filing
- Demonstration that results and correspondence are linked to the correct patient and encounter, not just saved in a generic inbox

MINIMUM FOR DEVELOPING

- Incoming information is filed into patient records but there is no formal process to confirm the clinician has reviewed it before filing - it may sit unactioned

EXCELLING

- The practice tracks turnaround time for reconciliation of incoming results and correspondence, and has escalation processes for critical or abnormal results that remain unacknowledged

COMMON PITFALLS

- Investigation results arrive electronically but sit in a system inbox that nobody monitors regularly - abnormal results can be missed for days or weeks
- Discharge summaries from hospitals are received but not reviewed by the specialist, so medication changes made during an admission are not reflected in the specialist'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.

ESTABLISHED EVIDENCE

- Completed clinical record audit reports (at least one within the past 12 months) covering a sample of records assessed against documented criteria (e.g., completeness of demographics, medication lists, allergy status, management plans)
- Evidence that audit findings were shared with clinicians - meeting minutes, written feedback, or audit summary distributed to the clinical team
- Documented actions taken in response to audit findings (e.g., template modifications, clinician education, repeat audit of identified gaps)

MINIMUM FOR DEVELOPING

- An informal review of records has been undertaken but it was not structured, documented, or followed by specific improvement actions

EXCELLING

- Record audits are scheduled on a recurring cycle (e.g., biannual), use consistent criteria, track trends over time, and feed into the practice's quality improvement plan

COMMON PITFALLS

- The practice conducted an audit once for accreditation purposes but has not repeated it - it was a point-in-time exercise, not an ongoing quality activity
- Audit findings identified significant gaps but no actions were taken, making the audit a wasted exercise

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.

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.

ESTABLISHED EVIDENCE

- A current, patient-facing privacy policy that describes how the practice collects, holds, uses, and discloses personal and health information
- Evidence of availability: published on the practice website, displayed or available in hard copy at reception, or included in the new patient intake pack
- The policy references the Australian Privacy Principles and includes the practice's contact details for privacy enquiries or complaints

MINIMUM FOR DEVELOPING

- A privacy policy exists but it is a generic template that has not been tailored to the practice's actual information handling practices, or it is not readily accessible to patients

EXCELLING

- The privacy policy is reviewed annually (with the review date noted on the document), updated when information handling practices change, and written in plain language appropriate for the patient population

COMMON PITFALLS

- The practice downloaded a template privacy policy years ago and has never updated it - it may reference legislation that has been amended or describe practices the practice no longer follows
- The policy exists on the website but reception staff do not know where it is and cannot direct patients to it when asked

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.

ESTABLISHED EVIDENCE

- A privacy collection notice provided to patients at or before their first consultation - either as a standalone document, a section of the intake form, or signage in the waiting area
- The notice explains what information is collected, why, who it may be shared with (e.g., referring GP, Medicare, private health insurers, other treating practitioners), and the patient's right to access and correct their records
- Evidence that the notice is actually provided - e.g., it is part of the standard intake process, included in the new patient pack, or displayed prominently

MINIMUM FOR DEVELOPING

- Some information is provided verbally by reception staff but there is no written notice, and the content varies depending on who is on the desk

EXCELLING

- The practice has tailored its collection notice to address specialty-specific sensitivities (e.g., mental health records, genetic information, fertility treatment records) and reviews it when the scope of information sharing changes

COMMON PITFALLS

- The intake form asks patients to sign a blanket consent to "share information as needed" without specifying who information may be shared with or for what purpose - this does not satisfy the APP 5 notification requirement
- Patients referred from hospitals assume the specialist already has all their information and are not told what additional information will be collected or how it will be used

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.

ESTABLISHED EVIDENCE

- Review of the practice's intake forms and data collection practices confirms that only information directly related to clinical care and practice administration is collected
- The practice can articulate why each piece of information it collects is necessary - there is a rational connection between what is asked and what is needed
- No collection of information that is irrelevant to the practice's functions (e.g., unnecessary demographic detail, social information not related to clinical care)

MINIMUM FOR DEVELOPING

- The practice has not reviewed its intake forms or data collection practices against the collection limitation principle - it collects what it has always collected without questioning necessity

EXCELLING

- The practice periodically reviews its intake forms and data collection processes to remove fields that are no longer necessary, and documents the rationale for any sensitive information collected

COMMON PITFALLS

- Intake forms collect information "just in case" - for example, detailed occupational history for a dermatology practice where it is rarely clinically relevant
- Third-party intake form platforms collect data beyond what the practice needs, and the practice has not reviewed what the platform collects or retains

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.

ESTABLISHED EVIDENCE

- A documented policy or procedure setting out when patient information may be disclosed, distinguishing between disclosure with consent, disclosure authorised by law, and disclosure required by law
- Evidence that staff have been trained on the distinction - for example, training records, meeting minutes, or a quick-reference guide available to reception and clinical staff
- Examples of how the practice handles common disclosure scenarios: requests from family members, requests from insurers, subpoenas, mandatory notifications

MINIMUM FOR DEVELOPING

- Staff generally understand that they should not share patient information without permission, but there is no written policy and staff are unsure how to handle edge cases (e.g., a parent requesting records for an adult child, an insurer requesting clinical notes)

EXCELLING

- The practice maintains a log of disclosure decisions for non-routine requests (e.g., subpoenas, statutory authority requests) and reviews these periodically to identify training needs or policy gaps

COMMON PITFALLS

- Reception staff provide clinical information to a caller claiming to be a family member without verifying the patient's consent - this is a common and serious breach
- The practice discloses more information than necessary when responding to a subpoena, providing the entire clinical record rather than only the documents specified

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.

ESTABLISHED EVIDENCE

- A documented process for handling patient access requests under APP 12, including who receives the request, how it is logged, the timeframe for response (30 days), and how records are provided (electronically, hard copy, supervised access)
- A log or register of access requests received, showing the date of request, date of response, and what was provided
- Evidence that where access has been refused (rare), the reason was documented and the patient was informed of their right to complain to the OAIC

MINIMUM FOR DEVELOPING

- Access requests are handled ad hoc by whoever receives them, with no formal process or tracking of response times

EXCELLING

- The practice tracks response times for access requests and reviews the data to ensure compliance with the 30-day requirement, identifying and addressing any bottlenecks

COMMON PITFALLS

- The practice charges excessive fees for providing copies of records, deterring patients from exercising their access rights - fees must not be excessive and must not apply to the request itself
- Requests are delayed because the treating clinician wants to "review" the notes before release, adding weeks to the process without a lawful basis for withholding access

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.

ESTABLISHED EVIDENCE

- A documented process for handling patient requests to correct their health records under APP 13, including how corrections are made as amendments (not deletions), how the original entry is preserved, and how the patient is notified of the outcome
- De-identified example showing how a correction appears in the clinical record - the original entry intact with the amendment clearly marked, dated, and attributed
- Evidence that staff understand they must not delete or overwrite original entries when making corrections

MINIMUM FOR DEVELOPING

- Corrections are made when requested but there is no written process, and staff are unsure whether they should delete the original entry or add an amendment

EXCELLING

- The practice proactively informs patients of their right to request corrections (e.g., in the privacy collection notice) and tracks correction requests to identify recurring data quality issues

COMMON PITFALLS

- A clinician "fixes" an error by deleting the original entry and rewriting it - this destroys the audit trail and may constitute a breach of record-keeping obligations
- The practice refuses a correction request without documenting the reason or informing the patient of their right to attach a statement to the record

5.3 — Data Security

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

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).

ESTABLISHED EVIDENCE

- A user access register listing all active accounts, the person assigned to each account, their role, and their access level within the clinical system
- Documentation of the role-based access model showing that access levels are differentiated (e.g., reception staff can view demographics and appointments but not full clinical notes; clinicians have full clinical access; billing staff have billing access)
- Confirmation that no shared login accounts exist - each user has their own credentials

MINIMUM FOR DEVELOPING

- Individual logins are in place but access levels have not been differentiated - everyone has the same level of access regardless of role

EXCELLING

- The user access register is reviewed at least annually, access levels are adjusted when roles change, and the review is documented with sign-off by the practice manager

COMMON PITFALLS

- A "reception" login is shared between three front-desk staff - this means no individual accountability and no way to trace who accessed a particular record
- Clinicians have full administrative access to the system, including the ability to delete records, modify audit trails, or change system settings

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.

ESTABLISHED EVIDENCE

- A password policy specifying minimum complexity requirements (length, character types), prohibiting password reuse, and defining change frequency
- Evidence that multi-factor authentication (MFA) is enabled for clinical systems where supported, and for all remote access (e.g., VPN, cloud-hosted clinical software accessed from home)
- Confirmation that default passwords on clinical systems, network devices, and peripherals have been changed

MINIMUM FOR DEVELOPING

- Passwords are in use but there is no formal policy, complexity is not enforced by the system, and MFA is not enabled despite being available

EXCELLING

- The practice uses a password manager for shared service accounts (e.g., practice-level logins to pathology ordering portals) and conducts periodic checks that MFA is active on all applicable systems

COMMON PITFALLS

- Passwords are written on sticky notes attached to monitors or stored in a shared document labelled "passwords" on the desktop - this is extraordinarily common in specialist practices
- MFA is available on the clinical software but was never enabled because "it's too inconvenient" - convenience does not override the obligation to take reasonable steps to protect health information

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.

ESTABLISHED EVIDENCE

- An offboarding checklist or procedure that includes revocation of system access on the day of departure, covering clinical software, email, network access, remote access, and any third-party systems (e.g., pathology ordering, My Health Record)
- Evidence of timely execution: access revocation records or IT service requests dated on or before the staff member's last day
- An annual review of active user accounts, documented, confirming that no dormant or orphaned accounts remain active

MINIMUM FOR DEVELOPING

- Access is generally revoked when staff leave but there is no formal checklist, and the process relies on someone remembering to do it

EXCELLING

- The practice conducts quarterly reviews of active accounts (not just annual) and cross-references against the current staff list, with discrepancies investigated and resolved

COMMON PITFALLS

- A registrar who rotated out six months ago still has active login credentials because nobody remembered to deactivate the account - this is a data breach waiting to happen
- Role changes (e.g., a nurse moving from clinical to administrative duties) do not trigger a review of access levels, leaving the person with clinical access they no longer need

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.

ESTABLISHED EVIDENCE

- Evidence that workstations used to access clinical records are configured to lock automatically after a defined period of inactivity (e.g., 5 minutes)
- Documentation of physical security measures: workstations are not visible to patients, screens face away from public areas, and consultation rooms are locked when unattended
- For mobile devices (laptops, tablets, phones) used to access patient information: evidence of device encryption, passcode or biometric lock, and remote wipe capability

MINIMUM FOR DEVELOPING

- Workstations have screen locks but the timeout is set too long (e.g., 30 minutes) or is inconsistently applied across devices

EXCELLING

- The practice maintains a register of all devices authorised to access clinical systems, including mobile devices, and reviews the register when staff join or leave

COMMON PITFALLS

- A clinician accesses patient records on a personal laptop that is not encrypted and is also used by family members - this is a significant breach risk
- Computer screens in reception or nursing stations are visible to patients in the waiting area, exposing the records of other patients

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.

ESTABLISHED EVIDENCE

- Documentation of the practice's IT security measures: firewall, antivirus/anti-malware software, and evidence that these are current (subscription active, definitions updated)
- Evidence that operating systems and clinical software are kept up to date with security patches - update logs or managed service reports
- A nominated person or IT provider responsible for security, with contact details and scope of responsibility documented

MINIMUM FOR DEVELOPING

- Antivirus software is installed but the practice is unsure whether it is current, and there is no IT support arrangement - security is managed on an ad hoc basis by whoever knows the most about computers

EXCELLING

- The practice has a managed IT services agreement that includes proactive security monitoring, patch management, and regular security assessments, with reports reviewed by the practice manager

COMMON PITFALLS

- The practice runs clinical software on Windows machines that are no longer receiving security updates - this is an unacceptable risk for systems holding health information
- The practice Wi-Fi network used by staff to access clinical systems is the same network provided to patients in the waiting room, with no segmentation

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.

ESTABLISHED EVIDENCE

- Paper records (where they still exist) are stored in locked cabinets or a secure records room with access restricted to authorised staff
- A process for managing records in transit - e.g., files moved between consultation rooms are not left unattended in corridors, and records sent to off-site storage are transported by a secure provider
- An index or tracking system so that the location of any given paper file can be determined

MINIMUM FOR DEVELOPING

- Paper records are stored in a dedicated area but filing cabinets are not locked, or the storage room is accessible to all staff including those who do not need records access

EXCELLING

- The practice has a plan and timeline for digitising remaining paper records, with progress tracked and prioritisation based on clinical need (e.g., active patients first)

COMMON PITFALLS

- Old paper records are stored in cardboard boxes in a storeroom that is also used for general supplies - no index, no lock, and water damage waiting to happen
- Paper records are left on desks or in consultation rooms overnight, accessible to cleaning staff or anyone who enters the premises after hours

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.

ESTABLISHED EVIDENCE

- Documentation of the clinical software vendor's security arrangements, including: where patient data is hosted (Australia or overseas), whether data is encrypted at rest and in transit, the vendor's data breach notification obligations, and their backup and disaster recovery arrangements
- Evidence that this information has been obtained - vendor security questionnaire, contract clauses, or correspondence with the vendor
- The vendor agreement addresses data ownership, data portability (ability to extract your data), and what happens to data if the vendor relationship ends

MINIMUM FOR DEVELOPING

- The practice uses a well-known clinical software product but has never asked the vendor about its security arrangements or reviewed the relevant clauses in the agreement

EXCELLING

- Vendor security is reviewed annually or when the vendor notifies of changes, and the practice has assessed whether its vendor's arrangements meet the requirements of APP 11

COMMON PITFALLS

- The practice assumes that because the clinical software is "cloud-based" it must be secure - cloud hosting does not automatically mean the vendor has adequate security controls
- The vendor agreement does not address data portability, meaning the practice could lose access to years of clinical records if it changes software

5.4 — Backup and Disaster Recovery

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

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.

ESTABLISHED EVIDENCE

- Documentation of the backup schedule showing automated backups occur at least daily, including what is backed up (clinical database, documents, attachments, templates, configuration)
- Backup logs or monitoring reports confirming that backups are completing successfully - not just scheduled but verified
- For cloud-hosted clinical software: vendor documentation or correspondence confirming their backup schedule, frequency, and scope

MINIMUM FOR DEVELOPING

- Backups are configured but nobody checks whether they are completing successfully - the last verification was months ago, if ever

EXCELLING

- Backup success is monitored daily (via automated alerts or a managed service), and backup failures trigger an immediate investigation and resolution process

COMMON PITFALLS

- The backup job has been failing silently for weeks because the backup drive is full or disconnected, and nobody noticed because no one checks
- The practice backs up the clinical database but not the attached documents (scanned letters, investigation results, images), which would be lost in a recovery scenario

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.

ESTABLISHED EVIDENCE

- Documentation confirming that backups are stored in a location physically separate from the primary system - cloud storage, off-site data centre, or removable media stored at a different premises
- Confirmation that backups are encrypted, both in transit and at rest
- If removable media is used, evidence of a process for secure transport and storage (not left in a car or at a staff member's home without protection)

MINIMUM FOR DEVELOPING

- Backups are stored on a separate device (e.g., external hard drive) but at the same premises as the primary system, providing no protection against fire, flood, or theft

EXCELLING

- The practice uses a 3-2-1 backup strategy (three copies, two different media types, one off-site) and documents the configuration, with encryption verified periodically

COMMON PITFALLS

- The backup hard drive sits under the reception desk, next to the server it is backing up - if the premises are damaged, both are lost
- Backups are stored in the cloud but the encryption key is unknown, or the cloud account uses a weak password without MFA

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.

ESTABLISHED EVIDENCE

- A documented record of backup restoration testing, performed at least once in the past 12 months, confirming that clinical data can actually be recovered from backups
- The test record includes the date, who performed it, what was restored (full or partial), how long it took, and whether the restored data was complete and usable
- If the test identified issues (e.g., corrupted backups, slow restoration, missing data), evidence of corrective actions taken

MINIMUM FOR DEVELOPING

- The practice understands that backups should be tested but has not yet performed a restoration test - it is relying on faith that the backups work

EXCELLING

- Restoration tests are conducted more frequently than annually (e.g., six-monthly), include different recovery scenarios (full system failure, single file recovery), and the results inform updates to the business continuity plan

COMMON PITFALLS

- The practice says "our IT guy handles it" but there is no documented evidence that a restoration test has been performed - an IT provider claiming backups are fine is not the same as a tested recovery
- The backup was tested once when the system was first set up three years ago, and no test has been done since despite the data volume growing significantly

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.

ESTABLISHED EVIDENCE

- A documented business continuity plan that addresses how the practice will operate if its clinical system becomes unavailable, covering: how patients will be seen (paper-based fallback), how critical clinical information will be accessed (e.g., printed medication lists, emergency contact lists), who activates the plan, and communication protocols for staff and patients
- Evidence that the plan covers multiple scenarios: IT system failure, ransomware attack, internet outage, vendor system outage, and physical events (fire, flood)
- Evidence that relevant staff know the plan exists and understand their role in it - training record, meeting minutes, or tabletop exercise

MINIMUM FOR DEVELOPING

- The practice has thought about what it would do if systems went down but has not documented anything - the plan exists only in the practice manager's head

EXCELLING

- The business continuity plan has been tested through a tabletop exercise or simulated outage within the past 12 months, with lessons learned documented and incorporated into a revised plan

COMMON PITFALLS

- The plan assumes the internet will always be available for cloud-hosted software - it does not address what happens during an internet outage, which can be caused by something as mundane as a severed cable
- Nobody knows where the plan is, and the only person who understands the IT infrastructure is an external IT contractor with no after-hours contact arrangement

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.

ESTABLISHED EVIDENCE

- Documented recovery time objective (RTO) - how long the practice can operate without its clinical system before patient care is materially compromised - and recovery point objective (RPO) - how much data the practice can afford to lose (e.g., one hour, one day)
- Evidence that these objectives are realistic and based on the practice's actual clinical operations, not aspirational targets
- Evidence that the backup and recovery arrangements are aligned with the stated objectives (e.g., if the RPO is one hour, backups must run at least hourly)

MINIMUM FOR DEVELOPING

- The practice has not formally defined RTO and RPO but has a general sense that "we need to be back up within a day or so"

EXCELLING

- RTO and RPO are reviewed annually, tested against the actual backup and recovery capability, and updated when the practice's operations change (e.g., new locations, increased patient volume, move to cloud software)

COMMON PITFALLS

- The practice states an RTO of four hours but its backup restoration process takes two days - the objective is meaningless if the capability does not match
- RPO is set at 24 hours (daily backup) but the practice sees 40 patients a day - losing a full day of clinical notes is a significant patient safety issue that has not been properly considered

5.5 — Secure Communication

We transmit patient information securely and appropriately.

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.

ESTABLISHED EVIDENCE

- Documentation of the secure messaging platform(s) used by the practice for clinical correspondence (e.g., Medical Objects, Argus, HealthLink, ReferralNet)
- Evidence that the secure messaging system is integrated with the clinical software and is the default channel for sending referral letters, reports, and results to other providers
- Confirmation that the majority of outgoing clinical correspondence is transmitted via secure messaging rather than standard email, fax, or post

MINIMUM FOR DEVELOPING

- A secure messaging system is installed but is not consistently used - some clinicians still default to email or fax for clinical correspondence

EXCELLING

- The practice monitors the proportion of correspondence sent via secure messaging versus insecure channels, and actively works to increase secure messaging adoption among its referral network

COMMON PITFALLS

- The secure messaging system is configured but incoming messages are not being downloaded or actioned because nobody checks the inbox - it is a one-way channel
- The practice sends correspondence via secure messaging but receives replies by fax because the referring GP has not adopted electronic messaging - the practice has not followed up to encourage the switch

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.

ESTABLISHED EVIDENCE

- A documented policy on the use of email for patient-identifiable information, specifying when email may be used, what safeguards must be applied (e.g., encryption, password-protected attachments, confirmed recipient address), and when email must not be used
- Evidence that staff have been trained on the policy and understand that standard unencrypted email is not a secure channel for health information
- Where email is used for clinical communication, evidence of applied safeguards (e.g., email encryption enabled, use of encrypted file-sharing platforms, confirmation of recipient address before sending)

MINIMUM FOR DEVELOPING

- There is an informal understanding that "you shouldn't email patient information" but no written policy, and staff occasionally email clinical documents because it is faster than alternatives

EXCELLING

- The practice has implemented technical controls (e.g., email encryption by default, data loss prevention rules that flag outgoing emails containing patient identifiers) in addition to policy-based controls

COMMON PITFALLS

- The practice manager uses their personal Gmail account to email clinical documents because "the practice email is too slow" - personal email accounts have no place in clinical communication
- Patient-identifiable information is emailed to the correct recipient but a CC or BCC is accidentally included, disclosing the information to an unintended party

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).

ESTABLISHED EVIDENCE

- A documented assessment of fax use in the practice, identifying what is sent by fax, to whom, and the risks associated with each use case
- Where fax remains in use, documented safeguards: programmed speed dials to prevent misdialling, confirmation of the recipient's fax number before sending, cover sheets marked "confidential," and verification of receipt for sensitive documents
- Evidence that the practice has considered whether fax can be replaced by secure electronic alternatives, with a documented decision

MINIMUM FOR DEVELOPING

- Fax is still used routinely but the practice has not formally assessed the risk or implemented specific safeguards beyond general care

EXCELLING

- The practice has eliminated fax for clinical correspondence and can demonstrate the transition to secure electronic alternatives, with fax retained only where external parties require it and with documented safeguards

COMMON PITFALLS

- Fax numbers are manually entered each time, without verification - misdirected faxes containing clinical information are a frequent source of privacy complaints to the OAIC
- The practice's fax machine is in a shared area accessible to all staff and visitors, and received faxes sit in the tray until someone collects them

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.

ESTABLISHED EVIDENCE

- A documented policy governing which channels may be used for patient communication (SMS, email, patient portal, messaging apps), what information may be communicated through each channel, and the requirement for patient consent to use that channel
- Evidence that patient consent to the communication channel is obtained and recorded - e.g., a field on the intake form, a notation in the patient record
- The policy addresses common scenarios: appointment reminders, results notification, billing communications, and clinical advice

MINIMUM FOR DEVELOPING

- The practice uses SMS for appointment reminders but has no written policy on what other information can be sent via SMS, and has not considered patient consent for each channel

EXCELLING

- The practice regularly reviews its patient communication channels against emerging privacy guidance (e.g., OAIC recommendations on health information in SMS and email) and updates its policy accordingly

COMMON PITFALLS

- Clinical results are communicated via SMS with the result included in the message body - if the phone is shared or lost, sensitive health information is exposed
- Staff use personal WhatsApp or iMessage to communicate with patients because it is convenient, without any policy, consent, or record of the communication in the clinical record

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.

ESTABLISHED EVIDENCE

- A documented process for verifying the identity of a person requesting patient information by phone, specifying what identifying information must be confirmed (e.g., full name, date of birth, address, Medicare number) and how many identifiers are required
- The process addresses different caller types: the patient themselves, a family member or carer, another health provider, and a third party (insurer, lawyer, government agency)
- Evidence that reception and clinical staff have been trained on the verification process and understand that clinical information must not be disclosed to unverified callers

MINIMUM FOR DEVELOPING

- Staff generally ask the caller's name before providing information but there is no formal verification process and no requirement for multiple identifiers

EXCELLING

- The practice uses a callback process for sensitive information requests (calling the patient or provider back on a verified number) and logs phone disclosure requests for audit purposes

COMMON PITFALLS

- A caller says "I'm Dr Smith's receptionist, can you fax the notes?" and the information is sent without verifying that the request is legitimate or that the fax number belongs to that practice
- The practice discloses appointment details to a caller claiming to be a spouse, without checking whether the patient has consented to information being shared with family members - this is particularly dangerous in family violence situations

5.6 — My Health Record

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

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).

ESTABLISHED EVIDENCE

- Confirmation of the practice's registration as a participating healthcare provider organisation in the My Health Record system, including the HPI-O (Healthcare Provider Identifier - Organisation) used for access
- If the practice has chosen not to participate, a documented decision recording the rationale and the implications understood (e.g., inability to view shared health summaries, inability to upload clinical documents)
- Evidence that the registration is linked to the practice's clinical software and that the My Health Record integration is technically functional

MINIMUM FOR DEVELOPING

- The practice is registered but the My Health Record integration has not been configured in the clinical software, so participation is nominal rather than active

EXCELLING

- The practice periodically verifies its registration details, confirms that the responsible officer and organisation maintenance officer contacts are current, and tests that the My Health Record integration is functioning correctly

COMMON PITFALLS

- The practice registered for My Health Record when it was set up years ago but the responsible officer has since left and nobody has updated the registration - the practice may be unable to manage its access if an issue arises
- The HPI-O is registered but the clinical software integration was never completed, so the practice cannot actually view or upload to My Health Records

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.

ESTABLISHED EVIDENCE

- Training records showing that staff who access the My Health Record system have been trained on their obligations under the My Health Records Act 2012, including: permitted purposes for access, prohibition on unauthorised access (including "curiosity" access), penalties for misuse, and the patient's right to set access controls
- Training covers both clinical and administrative staff who may interact with the system
- Training has been delivered within the past two years, or on commencement for new staff

MINIMUM FOR DEVELOPING

- Some staff have a general awareness of My Health Record but formal training has not been provided, and staff are unsure about the specific legal obligations

EXCELLING

- Training is refreshed annually, includes case studies relevant to the specialty (e.g., handling sensitive mental health or sexual health records in the context of My Health Record access controls), and is documented with attendance records

COMMON PITFALLS

- Staff access a patient's My Health Record out of curiosity (e.g., a colleague, a celebrity) without a clinical need - this is an offence under the Act with significant penalties
- The practice assumes that completing the initial My Health Record registration satisfies training requirements - registration and training are separate obligations

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.

ESTABLISHED EVIDENCE

- Documentation or screenshots showing that the clinical software is configured to upload relevant clinical documents to patients' My Health Records (e.g., specialist letters, event summaries, discharge summaries)
- Evidence that uploads are occurring - logs, reports, or spot-checks confirming that documents are being uploaded to patients' My Health Records when appropriate
- Configuration reflects the practice's specialty - the types of documents uploaded are relevant to the care provided (e.g., a cardiologist uploads specialist letters and diagnostic reports, not just generic event summaries)

MINIMUM FOR DEVELOPING

- The clinical software has My Health Record capability but uploads are not configured or are configured but not actually happening

EXCELLING

- The practice periodically audits My Health Record uploads to confirm accuracy and completeness, and has a process for correcting or removing documents uploaded in error

COMMON PITFALLS

- Uploads are configured to occur automatically but nobody has checked what is being uploaded - irrelevant or incomplete documents may be appearing in patients' My Health Records
- The configuration was set up for a previous version of the clinical software and broke during an upgrade - nobody noticed because no one checks

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.

ESTABLISHED EVIDENCE

- Evidence that clinicians check patients' My Health Records where it would support safe clinical care - particularly at first consultations, when prescribing, and when managing patients with complex medication regimens or multiple providers
- Clinical workflow or protocol that includes a prompt to check My Health Record at relevant consultation points
- De-identified examples or clinician attestation that My Health Record information (e.g., shared health summaries, medication lists, allergy information) is reviewed and considered in clinical decision-making

MINIMUM FOR DEVELOPING

- Some clinicians occasionally check My Health Record but it is not part of the routine clinical workflow and is done inconsistently

EXCELLING

- My Health Record review is embedded in the clinical workflow (e.g., automated prompt in the clinical software at the start of each new patient consultation) and clinicians document in their notes when MHR information has informed their clinical assessment

COMMON PITFALLS

- The practice is registered and uploads documents but never checks incoming information from other providers - My Health Record is treated as a one-way upload, not a shared clinical resource
- Clinicians do not check My Health Record before prescribing, missing medication interactions or allergy information that was available in the shared health summary

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.

ESTABLISHED EVIDENCE

- A documented process for managing patient requests that information not be uploaded to their My Health Record, including who receives the request, how it is actioned in the clinical software, and how it is recorded in the patient's file
- A process for identifying and managing situations where incorrect information has been uploaded to a patient's My Health Record, including how to request removal or correction through the My Health Record system
- Evidence that staff know how to action these requests - training records or a reference guide

MINIMUM FOR DEVELOPING

- Staff are aware that patients can restrict My Health Record access but are unsure how to action a restriction request in the clinical software or through the My Health Record system

EXCELLING

- The practice proactively asks patients with sensitive conditions (e.g., mental health, sexual health, genetic conditions) whether they have any concerns about information appearing in their My Health Record, and documents their preferences

COMMON PITFALLS

- A patient asks that a specific consultation not be uploaded but the request is not communicated to the clinician or actioned in the software, and the document is uploaded anyway
- The practice does not know how to remove a document that was uploaded to My Health Record in error - the process requires action through the My Health Record system operator, not just deletion from the local clinical record

5.7 — Record Retention and Disposal

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

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.

ESTABLISHED EVIDENCE

- Documentation showing the practice understands the applicable retention requirements: at least seven years from the date of last entry for adult records, and until the patient turns 25 (or seven years from last entry, whichever is later) for minors
- Evidence that the practice has identified the specific requirements for its jurisdiction, as some states and territories impose longer periods or additional requirements for certain record types (e.g., radiation treatment records, surgical records, mental health records)
- The practice can demonstrate that no records have been disposed of before the minimum retention period has elapsed

MINIMUM FOR DEVELOPING

- The practice has a general awareness that records must be kept "for years" but has not identified the specific legal requirements for its jurisdiction or specialty

EXCELLING

- The practice maintains a reference document mapping retention requirements to each record type it holds, updated when legislation or guidelines change, and shared with relevant staff

COMMON PITFALLS

- The practice applies the seven-year adult rule uniformly without considering that records for patients who were minors at the time of treatment must be retained until the patient turns 25 - disposing of paediatric records after seven years is a breach
- The practice does not account for jurisdiction-specific requirements, such as longer retention periods for records involving radiation or controlled substances

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.

ESTABLISHED EVIDENCE

- A documented retention schedule listing each category of record the practice holds, the applicable retention period, and the legislative or guideline reference for that period
- The schedule covers clinical records, imaging, pathology results, financial records, employment records, and any other categories relevant to the practice
- The schedule is accessible to staff responsible for records management and is reviewed when legislation changes

MINIMUM FOR DEVELOPING

- The practice knows the general retention period for clinical records but has not documented a schedule and has not considered retention periods for non-clinical records (financial, employment, compliance)

EXCELLING

- The retention schedule includes automated alerts or reminders when records approach the end of their retention period, triggering a review and disposal decision process

COMMON PITFALLS

- The schedule covers clinical records but ignores financial records (which the ATO requires to be kept for five years) or employment records (which have their own retention requirements under workplace legislation)
- The schedule exists but nobody follows it - records are neither reviewed nor disposed of, and the practice accumulates data indefinitely without purpose

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.

ESTABLISHED EVIDENCE

- A documented process for secure disposal of records that have reached the end of their retention period, specifying the method: shredding or certified document destruction for paper records, and permanent deletion (not just "moving to trash") for electronic records
- Disposal records: certificates of destruction from document destruction services, or logs recording what was destroyed, when, and by whom
- For electronic records, evidence that the disposal method prevents data recovery (e.g., secure deletion software, physical destruction of storage media)

MINIMUM FOR DEVELOPING

- Paper records are shredded in-house but there is no log of what was destroyed, and electronic record disposal has not been considered

EXCELLING

- The practice uses a certified document destruction provider for paper records and has validated that its electronic deletion process meets the requirements of APP 11.2, with destruction certificates retained as part of the compliance record

COMMON PITFALLS

- Paper records are placed in general waste or recycling bins rather than securely shredded - this is a notifiable data breach
- Electronic records are "deleted" from the clinical software but remain in database backups indefinitely, meaning they are never truly disposed of - the practice has not considered how to purge old data from backups

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.

ESTABLISHED EVIDENCE

- A documented plan for the custody and management of clinical records in the event of practice closure, practitioner retirement, or practitioner departure, addressing: who will assume custody, how patients will be notified, how records will be transferred, and how retention obligations will continue to be met
- Evidence that the plan includes giving patients reasonable notice and the opportunity to nominate where their records should be sent
- If a practitioner has already departed, evidence that the plan was followed - patient notifications sent, records transferred to the nominated custodian, and the arrangement documented

MINIMUM FOR DEVELOPING

- The practice has not considered what would happen to records if it closed or a sole practitioner became incapacitated - there is no plan

EXCELLING

- The plan is reviewed annually, includes succession arrangements for the records custodian role, and addresses unexpected closure (e.g., death or incapacity of a sole practitioner) as well as planned closure

COMMON PITFALLS

- A practitioner leaves a group practice and takes "their" patient records on a USB drive with no formal transfer process, no patient notification, and no copy retained by the practice - this creates gaps in both locations
- A sole practitioner retires with no plan for records custody, leaving thousands of clinical records in an empty office or with a family member who has no understanding of privacy obligations

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.

ESTABLISHED EVIDENCE

- A documented policy or awareness statement confirming that records subject to a current or anticipated complaint, claim, investigation, or legal proceeding must not be disposed of, regardless of whether the retention period has passed
- Evidence that staff involved in records management understand the concept of a litigation hold and know to escalate before disposing of any records where there is a current or potential claim
- The policy specifies who has authority to impose and lift a litigation hold, and how affected records are flagged in the records system

MINIMUM FOR DEVELOPING

- There is a general understanding that "you shouldn't destroy records if there's a complaint" but no written policy or process for flagging and protecting relevant records

EXCELLING

- The practice has a proactive process for identifying records that may be subject to litigation hold - for example, checking with the practice's insurer or legal adviser before any bulk disposal of records, and maintaining a register of active complaints or claims with linked record identifiers

COMMON PITFALLS

- Records relating to an active AHPRA complaint are routinely destroyed because the retention period has passed and the person managing disposal is unaware of the complaint - this can constitute destruction of evidence
- The practice disposes of records after a complaint is resolved without checking whether an appeal or further claim is possible within the limitation period

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