Fraud & Risk Checklist.

A Practical Guide for GP Clinic Owners and Practice Managers to Minimise Employee Fraud.

Simplifying Payments, Permissions, and Compliance

Accounts Payable

- [ ] All supplier changes (BSB, account number, contact details) are verified through a TRIPLE-check process (voice, text, and email) before being updated in Xero/MYOB.

  Never update supplier bank details based on an email or phone call alone. Triple verification helps protect against AI-generated fraud.

- [ ] Dual approval is required for any payment above $_____.

  Avoid locking into long-term or long-dated service agreements. Keep contracts with suppliers or service providers to 12 months or less.

- [ ] Supplier invoices are matched to a purchase order or contract before payment, or approved by the person who can confirm receipt of goods/services.

- [ ] No single staff member can both set up and approve the same payment.

- [ ] The Xero/MYOB supplier listing is reviewed regularly (monthly or quarterly) by the practice owner or a second person to confirm accuracy and completeness.

- [ ] ABA payment files are prepared by one person (e.g., bookkeeper) and authorised in the banking portal by a separate person (e.g., practice owner).

  Applies to CBA NetBank, NAB Connect, Westpac Live, ANZ Internet Banking for Business, etc.

Payroll

- [ ] New employee setup and pay rate changes (including superannuation) are approved in writing by a second authorised person before being entered into payroll system.

- [ ] Payroll reports are approved by a second person before processing e.g., Practice Manager rosters & approves timesheets; bookkeeper or external payroll provider processes the payrun.

- [ ] The bank ABA file for payroll is approved by a second person, cross-checked against the payrun source data (timesheets, rosters, pay rates).

- [ ] Terminated employees are promptly removed from the payroll system, and their system access is revoked on their last day.

- [ ] Payroll spend is reviewed against budget and rosters regularly (at least monthly).

- [ ] Superannuation is paid via compliant commercial clearing houses or built-in payroll software features, and payment confirmations are reconciled.

  Payday Super commenced 1 July 2026, ensure you remit super on each pay day.

- [ ] Overtime and leave adjustments require written approval; leave balances are reconciled against the payroll system regularly.

Bookkeeping & Reporting

- [ ] Live bank feeds are connected in Xero/MYOB; manual CSV imports are not used for bank reconciliation.
  Manual imports create an opportunity for manipulation. Live feeds reduce this risk significantly.
- [ ] Bank reconciliations are completed regularly (daily/weekly) in accounting software, with an independent check performed regularly (e.g., accountant checks the monthly reconciliation during BAS preparation).
- [ ] Financial reports (P&L;, balance sheet, accounts receivable) are reviewed and approved monthly by the practice owner.
- [ ] Segregation of duties is in place, no single person prepares, approves, and reviews financial transactions.
- [ ] Credit card statements are reconciled against accounting records monthly, with all transactions reviewed by the practice owner.
- [ ] All direct debits are checked regularly. Unchecked direct debits are a common fraud vector raise a dispute with the bank immediately for any false or unauthorised direct debit.
- [ ] An external accountant or BAS-registered bookkeeper conducts a periodic independent review (at minimum quarterly).

Banking Structures & View-Only Account Access

- [ ] Online banking roles are configured so that staff who need to view statements (e.g., bookkeeper, receptionist) have View-Only or Enquiry-Only access, they cannot initiate or approve payments.
  In CBA NetBank Business, NAB Connect, Westpac Live, and ANZ IB for Business, user roles can be set to 'View Only' or 'Enquiry'. Confirm this is in place for all non-authorised users.
- [ ] Payment initiation (creating/uploading ABA files) and payment authorisation are assigned to different individuals in the banking portal.
- [ ] Do not delegate payment authorities below a threshold. All money movement requires proper approval, there should be no rules allowing individuals to move money independently up to a certain amount.
- [ ] Money movement is reviewed in a regular synchronous meeting (e.g., fortnightly via Zoom, without recording or transcription). Expect this to take 20-30 mins initially, dropping to 10-20 mins over time.
- [ ] The practice owner (or a second authorised signatory) is the sole person able to add or change payees/beneficiaries in the online banking system.
- [ ] A separate operating account is used for day-to-day receipts and payments; a separate savings or reserve account holds retained funds, with restricted access.
- [ ] Medicare and DVA bulk-billing payments are deposited into a practice-controlled bank account, not a personal or individual practitioner account, unless a formal tenant doctor arrangement is in place with documented controls.
  Recent changes by Tyro and HICAPS may require settlements to flow to an ABN-linked account. Confirm your arrangement with your terminal provider and accountant.
- [ ] Bank account details shown in accounting software (Xero/MYOB) are reconciled against actual bank statements at least quarterly. Any change to bank details must follow the TRIPLE check process.
- [ ] All bank account signatories are reviewed annually; former staff or directors are removed promptly.

Banking & Cash Handling

- [ ] No single person has full control of both cash handling and banking.
- [ ] Two staff members count all cash together at the end of each session or day.
- [ ] Cash is banked daily and reconciled to the PMS. Petty cash has no place in the practice.
- [ ] Consider using Weel (weel.com) prepaid cards instead of petty cash. Cards are preloaded and follow a hierarchical spending capacity for unplanned expenses (e.g., Reception ~$50, Practice Manager ~$500, Operations ~$5,000).

  The Weel app prompts for invoices/receipts and verifies the reason for spend. Cards are recharged monthly based on usage.
- [ ] EFTPOS/Tyro is integrated directly with the PMS — no manual entry of terminal totals is permitted.
- [ ] Cash variances are investigated and documented immediately, with a written explanation retained.

Payment Terminals & PMS Refund/Receipt Permissions

- [ ] Every staff member has their own unique PIN for each Tyro/HICAPS terminal, no shared PINs, no use of the clinic's postcode as a PIN.

  Shared PINs remove individual accountability and may void your business insurance policy. Contact Tyro or HICAPS to confirm individual PIN assignment.
- [ ] The 'Unmatched Refund' feature is disabled on all Tyro/HICAPS terminals, confirmed in writing from the terminal provider.

  Without this control, a refund can be issued to any card, not just the original paying patient. This is a primary mechanism for terminal fraud.
- [ ] All Tyro/HICAPS terminal transactions are reconciled against the PMS (Best Practice, MedicalDirector, Zedmed, Cliniko) daily; not just at month-end.

  Note: EFTPOS cash-outs, declined transactions, voided transactions, non-standard refunds, split payments, WorkCover/TAC payments, and NDIS payments may NOT automatically appear in the PMS and require manual reconciliation.
- [ ] In the PMS, the ability to process a refund or reverse a receipt is restricted to authorised staff only (e.g. Practice Manager or above); not available to all reception staff.

  In Best Practice: Security → User Groups → restrict 'Reverse Receipt' and 'Refund' permissions. In MedicalDirector: User Administration → Role Permissions. In Zedmed: Administration → User Security.
- [ ] A two-person check is required for all refunds and receipt reversals in the PMS; one person initiates, a second person (Practice Manager or owner) approves and signs off.
- [ ] The ability to change a patient's bank account details or Medicare card details in the PMS is restricted to authorised staff only.
- [ ] PMS audit logs (transaction history, receipt reversals, item number changes) are reviewed regularly by the practice owner or an independent person.
- [ ] Physical terminals are secured when not in use (e.g., locked to the counter or stored in a locked drawer overnight) to prevent theft or tampering.

Medicare & MBS Billing Controls

- [ ] Each doctor reviews and signs off on their own MBS item numbers billed for the day; a daily billing confirmation checklist is in place.

  The provider number holder is ultimately responsible to Medicare for all claims made under their number, even if submitted by staff.

- [ ] Changes to MBS item numbers after the day of consultation are restricted in the PMS and require written approval from the treating doctor.
- [ ] Regular reports are generated and reviewed to detect unusual changes in Medicare billing patterns (e.g., sudden increase in Level C/D consultations, or high volumes of specific item numbers).
- [ ] Bulk-billed patients are not also charged a gap or 'extras' payment, receipts are reconciled to confirm no double-dipping.
- [ ] The practice has a documented process for responding to a Medicare compliance audit or a Department of Health and Aged Care (DHAC) review.
- [ ] DVA, WorkCover, and third-party payer claims are reconciled against payments received and any outstanding amounts are followed up promptly.

System Access & Security

- [ ] All staff use individual logins for all systems, no shared accounts in the PMS, Xero/MYOB, banking portals, or Medicare PRODA/HPOS.
- [ ] Two-factor authentication (2FA) is enabled for all financial systems, including Xero, MYOB, online banking, and Medicare PRODA.
- [ ] Access permissions are based on role (least privilege principle); staff only have access to the functions required for their specific role.
- [ ] A formal access review is completed at least every six months; former staff are removed, and role appropriateness is confirmed for current staff.
- [ ] When a staff member is terminated or resigns, all system access (PMS, Xero/MYOB, banking, email, PRODA) is revoked on their last day.
- [ ] PRODA (Provider Digital Access) accounts are reviewed to ensure only current, authorised staff have access to Medicare Online and HPOS.

General Controls & Practice Culture

- [ ] Clear role separation is documented; who can prepare, approve, and review financial transactions is written down and communicated to all relevant staff.
- [ ] Key financial control policies are communicated to all staff at induction and reviewed annually.
- [ ] An external accountant or advisor (specialist in medical practices) conducts a periodic independent review of financial controls.
- [ ] The practice has a confidential reporting mechanism (e.g., direct line to the practice owner) for staff to raise concerns about suspicious financial activity.
- [ ] Practice carries appropriate business insurance, including fidelity/employee dishonesty cover, & the policy has been reviewed to confirm it covers the practice's specific arrangements (inc. terminal arrangements).

Personality Cues: High-Risk Senior Staff Profiles.

- [ ] Watch for excessive span of control: a senior staff member who is the only person with access to everything and never hands off control of email or money movement.
- [ ] Watch for staff who only ever take short holidays and still log in while on leave. These individuals are often described by owners as 'super helpful' and 'critical to the business'.
- [ ] ACTION: If you have a person matching this profile, review your financial controls immediately. The practice owner must take back control of money movement.
- [ ] ACTION: Reassign the ownership/admin status of all key software to the practice owners. (It is likely this person has assigned themselves owner status in all software; reverse this).
- [ ] ACTION: Slowly and carefully manage the risk before conducting a formal audit, as an abrupt audit may trigger the person if fraud is occurring.

Review Signoff.

Practice Name: _____ Date of Review: _____

Reviewed By: _____ Next Review Due: _____

Manager Signoff: _____

GROWTH MD
Specialist Medical Accountants.