CALEN HEALTH

Privacy, Confidentiality and Information Security Policy

Practice	Calen Health
Address	51 Hampden Road, Nedlands WA 6009
Policy owner	Dr Lisa O'Rourke – Privacy Officer
Operational privacy governance	Haylee Anastasi – Practice Manager
Clinical oversight	Dr Lisa O'Rourke / clinical leadership
IT / cybersecurity advisers	Jerome Chiew and Hugh Owens – Critical IT, Applecross
Applies to	All doctors, nurses, reception/administration staff, contractors, students, volunteers, temporary workers and other persons authorised to access Calen Health information or systems
Version	1.0
Effective date	18 September 2026
Review	At least annually and after significant incident, legislative/regulatory change, accreditation change, major system change or introduction of significant new technology

Purpose

Calen Health protects the privacy, confidentiality, security, accuracy and integrity of personal and health information. This policy establishes mandatory requirements for collection, access, use, disclosure, communication, storage, correction, transfer, retention and destruction. Technical ability to access information does not itself create authority to access it.

1. Regulatory framework

- Privacy Act 1988 (Cth) and Australian Privacy Principles (APPs), where applicable.
- Notifiable Data Breaches Scheme.
- My Health Records Act 2012 (Cth) and My Health Records Rules 2026.
- Healthcare Identifiers Act 2010 (Cth), where applicable.
- Medicare, Services Australia, PRODA and HPOS requirements.
- Applicable professional registration standards, codes of conduct and medical-record requirements.
- Applicable contractual, court, subpoena, mandatory reporting and other lawful disclosure requirements.
- RACGP information-management and privacy/security requirements applicable to the practice.

2. Core privacy rules

1. Access only information needed for an authorised task.
2. Being able to access information does not mean access is authorised.
3. Never look at a patient record out of curiosity.
4. Never access a friend, relative, colleague or known person's record without a legitimate authorised work reason.
5. Never share passwords, user accounts or authentication devices.
6. Lock screens whenever leaving a workstation unattended.
7. Verify the patient and recipient before sending or disclosing information.

8. Keep reception, telephone and clinical conversations discreet.
9. Never place identifiable patient information into unauthorised AI tools, personal email, personal messaging applications or personal devices.
10. Report mistakes, near misses and suspected breaches immediately and never conceal them.
11. Confidentiality continues after employment or engagement ends.
12. If uncertain, stop and seek guidance before accessing or disclosing.

3. Information covered

- Personal and health information, including demographics, contact details, Medicare/DVA and healthcare identifiers, medical histories, diagnoses, medications, allergies, pathology/imaging, referrals, correspondence, mental-health information, reproductive/sexual-health information, appointment information, billing/payment information and My Health Record information.
- Information received verbally, electronically, in writing, by telephone, SMS, email, portal, app, telehealth or AI-assisted documentation.
- Staff, contractor and practice operational information that is confidential.

4. Collection, use and disclosure

Calen Health will collect information reasonably necessary for healthcare and lawful practice operations. Patients will be informed, through the patient-facing Privacy Policy and relevant collection notices, about the purposes of collection, important service providers, access/correction rights, complaints and relevant overseas handling.

- Use and disclose information only for authorised healthcare, administrative, billing, communication, safety, legal, quality or other lawful purposes.
- Use the minimum information reasonably necessary.
- Verify identity and authority before releasing information.
- Escalate complex requests involving lawyers, police, subpoenas, insurers, government agencies, separated parents, deceased patients, guardianship/capacity, family violence or disputed authority.
- Do not use patient information for direct marketing except where lawful and authorised.

5. Best Practice Software

Best Practice Software is Calen Health's approved clinical practice-management/medical-record environment. It is the practice's primary clinical record for information entered into the practice record.

- Users must have individual accounts and role-appropriate permissions.
- Clinical records may be accessed only for legitimate authorised duties.
- Administrative staff must not open clinical information merely because the system permits access; access must be limited to what is necessary for their role.
- Users must not share credentials, leave sessions unattended, or bypass access controls.
- Clinical records must not be altered, deleted or exported outside authorised processes.
- Information copied from Best Practice to another system must have a legitimate purpose and be transferred only through an approved secure workflow.
- MHR information accessed through approved clinical software must be handled in accordance with the separate My Health Record Security and Access Policy.
- Identifiable information from Best Practice must not be entered into public/personal AI or transcription tools.

6. AutoMed Systems and AMS Connect

Calen Health will use AutoMed Systems and the AMS Connect mobile app for approved appointment booking, patient communications, digital forms and, where enabled, telehealth and payment workflows. AutoMed describes AMS Connect as its patient-facing mobile app and states that it integrates with Best Practice. Calen's current configuration and contracts determine which functions are activated.

- Only approved AutoMed/AMS workflows may be used for patient communications, forms, booking and related services.
- Staff must not export patient information from AutoMed to personal devices or unapproved applications.
- Digital forms and consents received through AutoMed must be handled as patient information and retained in the approved clinical record/workflow where required.
- SMS, email and app communications must contain only information appropriate to the communication channel and must follow patient communication preferences and applicable consent/opt-out controls.
- AutoMed access must use individual authorised accounts where supported and must be removed when no longer required.
- AutoMed is an external service provider; Calen remains responsible for its own privacy obligations and must not state that vendor liability replaces Calen's obligations.

7. Payments, credit cards and Tyro

Where AutoMed/AMS payment functions are enabled, patients may enter payment-card information through the approved payment workflow. Payment information is confidential personal information and must be protected.

- Staff must never write, photograph, screenshot, email, SMS or manually store a full card number (PAN), CVV/security code or equivalent card authentication data in Best Practice, AutoMed notes, paper records, spreadsheets or personal devices.
- Staff must use only the approved AutoMed/Tyro payment workflow for card-not-present payments and approved practice EFTPOS processes for card-present payments.
- Saved card/token arrangements, if enabled, must remain within the approved payment environment; staff must not create informal copies.
- Payment receipts, failed-payment messages and links must be checked before acting to reduce fraud and misdirection risk.
- Payment disputes, suspected fraud or exposure of card information must be escalated immediately to the Practice Manager and Critical IT where appropriate.

8. Lyrebird Health – AI clinical scribing

Lyrebird Health may be used as an approved AI-assisted clinical documentation tool. Calen will maintain a separate patient consent form and operational AI-scribe procedure.

- A patient's general treatment consent does not by itself constitute consent to AI scribing.
- Before first use, the patient must receive the separate Lyrebird consent information and provide written/digital consent.
- At the beginning of every clinical encounter in which Lyrebird is to be activated, the nurse or doctor must verbally confirm that the patient is comfortable with Lyrebird being used for that encounter.
- If the patient declines, withdraws consent or is uncertain, Lyrebird must not be activated and the consultation must be documented by the usual method.
- The clinician remains responsible for the clinical accuracy, completeness and appropriateness of the final note and must review it before it becomes part of the patient's clinical record.

- Only the Calen-approved Lyrebird account, device and workflow may be used.
- No identifiable patient information may be entered into personal/public AI systems.
- Calen will periodically verify Lyrebird's configured retention, processing location, access controls and contractual terms. Lyrebird currently states that Australian data is processed/stored in Australia, consultation audio is discarded after real-time transcription, and saved notes are encrypted with default seven-day retention; the practice's actual account settings and contractual terms control.

9. External providers

Approved external providers may include Best Practice, AutoMed/AMS Connect, Lyrebird Health, payment providers such as Tyro, IT/cybersecurity providers, pathology and imaging services, secure messaging providers, telecommunications providers, accounting/billing providers and Novopsych or similar external services used for patient-reported questionnaires or related clinical/psychological assessment workflows.

- Before introducing a new provider, Calen will consider the information handled, purpose, access, security controls, data location, retention, subcontractors, incident obligations and contractual arrangements.
- Where practicable, Calen will maintain a vendor register recording approved providers, services, data categories, data location and key privacy/security controls.
- Vendor contracts do not transfer Calen's own legal responsibilities. Incidents involving a vendor must be assessed and managed by Calen under its applicable obligations.

10. Access, correction and records

- Patients may request access to and correction of their personal information through the Privacy Officer or Practice Manager.
- Identity and authority must be verified before access is provided.
- Records must be retained and destroyed only in accordance with applicable legal and professional requirements.
- Where information is corrected, required audit integrity must be preserved.

11. Security controls

- Unique user identification and role-based access.
- Strong authentication and MFA where supported and appropriate.
- Secure passwords/password-management controls; no credential sharing.
- Automatic or manual screen locking when unattended.
- Secure remote access; no unauthorised remote-access software.
- Timely operating-system, application and security updates.
- Endpoint protection, firewall and network security appropriate to the practice environment.
- Encrypted transmission and secure storage where supported.
- Regular backups and tested information-recovery arrangements.
- Secure disposal of paper and electronic media.
- Physical security of workstations, servers, networking equipment and portable devices.
- Periodic access reviews and security-risk reviews with Critical IT.

12. Privacy and security incidents

All actual or suspected privacy, confidentiality or cybersecurity incidents must be reported immediately to the Practice Manager or Privacy Officer. The practice will contain the incident, preserve evidence, assess the information involved and determine applicable notification/escalation obligations, including the Notifiable Data Breaches Scheme and My Health Record requirements where relevant.

13. Governance and responsibilities

- Dr Lisa O'Rourke – Privacy Officer: privacy governance, privacy complaints, privacy policy oversight and escalation of significant privacy matters.
- Haylee Anastasi – Practice Manager / Responsible Officer: operational governance, access administration, staff training coordination, incident coordination and My Health Record governance.
- Jerome Chiew and Hugh Owens – Critical IT, Applecross: authorised IT/cybersecurity advisers responsible for agreed technical controls, monitoring, patching, backup/recovery support, incident technical response and security advice.
- Clinical leadership: clinical oversight of information handling and clinical documentation.
- Every staff member: individual responsibility to comply with this policy and report incidents.

14. Training

Privacy and information-security training is required at onboarding and periodically thereafter, with additional training following significant system, legislative, security or workflow changes. Training records will be maintained.

15. Review and document control

This policy will be reviewed at least annually and whenever significant risks, systems, legislation, accreditation requirements or technology change. Previous versions will be retained in accordance with applicable recordkeeping requirements.

Key source references

- My Health Records Rules 2026 (F2026L00392), Federal Register of Legislation.
- My Health Records Act 2012 (latest compilation C2026C00277, 1 July 2026).
- OAIC guidance on My Health Record security and access policies, updated September 2026.
- Current vendor information for AutoMed Systems, Lyrebird Health and other approved providers should be checked against Calen's actual contracts/configuration before implementation.