FCD Health Privacy, Confidentiality and Health Information Management Policy

Document control	Details
Document name	Privacy, Confidentiality and Health Information Management Policy
Document ID	FCD-PRV-001
Version	3.0
Authority	FCD Health Ltd
Responsible role	Chief Executive Officer
Applies to	All FCD Health services, workforce members, contractors, students and approved service providers
Review date	September 2027 or earlier if legislation, accreditation standards, systems or organisational risks change

1. Purpose

FCD Health is committed to protecting the privacy, confidentiality, integrity and appropriate availability of personal information and health information entrusted to the organisation. This policy establishes the organisation-wide requirements for collecting, using, disclosing, accessing, correcting, storing, securing, retaining and disposing of information across clinical, operational and corporate activities.

The policy supports safe clinical care, patient trust, lawful information handling, effective clinical handover, appropriate information sharing and continuous compliance with privacy, health information, accreditation and information-security obligations.

2. Scope

This policy applies across all FCD Health operated services and activities, including:

- Palmerston GP Super Clinic (PGPSC);
- Palmerston Medicare Urgent Care Clinic (PMUCC);
- Darwin Medicare Urgent Care Clinic (DMUCC);
- FCD Health GP Clinic (FCDHGPC);
- corporate, teaching, quality-improvement, research, outreach and other approved FCD Health activities.

It applies to employees, contractors, locums, visiting practitioners, students, registrars, volunteers, consultants and third-party service providers who access or handle FCD Health information.

This internal governance policy is supported by a separate patient-facing Privacy Policy / Privacy Notice written in plain English and made available through the FCD Health website and on request.

3. Legal, regulatory and accreditation framework

FCD Health manages privacy and health information in accordance with applicable obligations, including:

- Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs);
- the Notifiable Data Breaches scheme under the Privacy Act 1988 (Cth);
- Information Act 2002 (NT), where applicable to FCD Health activities or information exchanges;
- My Health Records Act 2012 (Cth) and associated rules where My Health Record is used;

- relevant professional confidentiality, consent, record-keeping and mandatory disclosure obligations;
- RACGP Standards for general practices, including confidentiality, privacy and information-security requirements;
- applicable ACHS, Medicare Urgent Care Clinic, funding, contractual and data-reporting requirements.

Where legislation or a binding contractual requirement imposes a higher standard than this policy, the higher requirement applies.

4. Core privacy principles

Principle	FCD Health requirement
Need to know	Access personal or health information only where required for an authorised role, task or clinical purpose.
Minimum necessary	Collect, use and disclose only the information reasonably necessary for the relevant purpose.
Transparency	Tell people, in a clear and accessible way, how and why information is collected, used, stored and disclosed.
Accuracy	Take reasonable steps to keep information accurate, complete, current and appropriately coded.
Security	Protect information against loss, misuse, interference, unauthorised access, modification and disclosure.
Confidentiality	Maintain confidentiality during clinical care, administration, teaching, meetings, handover and all verbal, written and digital communications.
Patient participation	Support patients to access and request correction of their information and to raise privacy concerns.
Accountability	Record, investigate, escalate and learn from privacy incidents, control failures and complaints.

5. Collection of personal and health information

FCD Health collects information necessary to provide healthcare, operate services, meet billing and funding requirements, communicate with patients and providers, conduct approved quality-improvement activities, meet legal obligations and manage the organisation.

Information should be collected directly from the patient where reasonably practicable. Information may also be received from carers, substitute decision-makers, other healthcare providers, hospitals, pathology or imaging services, government systems, referral partners or other authorised sources.

At or before collection, patients should be given appropriate information about the purpose of collection, usual uses and disclosures, how to access or correct information, and how to raise a privacy concern. Where practical and lawful, patients should be informed of options to interact anonymously or using a pseudonym, noting that this may not be compatible with safe clinical care, Medicare claiming, prescribing, pathology, referrals, statutory reporting or other identity-dependent services.

6. Use and disclosure

Personal and health information may be used or disclosed for the purpose for which it was collected, for a related purpose the person would reasonably expect where permitted by law, with consent, or where otherwise authorised or required by law.

Common authorised uses and disclosures include:

- providing, coordinating and handing over clinical care;
- referrals, pathology, imaging, pharmacy and specialist communication;
- billing, Medicare, funding and approved program reporting;
- recalls, reminders and clinically appropriate patient communications;
- clinical governance, incident review, complaints management, audit and quality improvement where authorised and appropriately controlled;
- mandatory reporting, court orders, subpoenas, statutory notices and other disclosures required or authorised by law;
- approved teaching, research or evaluation activities with the appropriate consent, ethics, legal and governance controls.

Staff must not disclose information to family members, friends, employers, insurers, lawyers, police, government agencies or other third parties unless the disclosure is authorised by the patient, permitted or required by law, or approved through the relevant FCD Health process.

7. Confidentiality in the practice environment

FCD Health must use reasonable physical, behavioural and workflow controls to protect confidentiality. Staff must:

- avoid discussing identifiable patient information in public areas or where conversations may be overheard;
- confirm identity before releasing information by telephone, email, portal, mail or in person;
- position screens and printed material to minimise unauthorised viewing;
- lock workstations when unattended and never share passwords or authentication credentials;
- use private clinical spaces for sensitive discussions wherever practicable;
- secure prescription stationery, labels, reports and other official documents;
- avoid accessing records of family, friends, colleagues, public figures or other persons unless access is required for authorised work;
- report suspected inappropriate access or disclosure immediately.

8. Clinical records and approved systems

FCD Health uses approved clinical, communication, booking, analytics, compliance and corporate systems. Each system must have an identified purpose, approved access arrangements and appropriate privacy, cybersecurity, contractual and data-governance controls.

Best Practice is the primary clinical record system. Secure messaging platforms such as HealthLink, Medical-Objects or other approved services should be used for clinical information exchange wherever available. HotDoc, Cubiko, My Health Record, PracticeHub and other approved systems may be used only for their authorised organisational purpose and in accordance with their approved configuration and FCD Health policy.

FCD Health must not represent that all third-party systems store or process data only in Australia unless this has been verified for the specific service, configuration and contract. Vendor privacy, hosting, subcontractor and cross-border arrangements must be assessed and documented before implementation and when materially changed.

9. Access controls and user management

- Each user must have a unique account where the system supports individual accounts.

- Access must be role-based and limited to the minimum information and functions necessary for the user's duties.
- Access for new starters, locums, students, contractors and temporary staff must be approved before use.
- Access must be reviewed when roles change and removed promptly when engagement ends.
- Privileged or administrative access must be restricted and monitored.
- Audit logs should be used where available to investigate suspected inappropriate access or other privacy concerns.

10. Telephone, email, SMS, portals and electronic communication

Electronic communication must balance accessibility with confidentiality and clinical safety. Staff must use approved channels and follow identity-verification and escalation processes appropriate to the sensitivity of the information.

- Do not send highly sensitive clinical information through ordinary email or SMS where a secure approved alternative is available.
- Confirm recipient details before sending referrals, reports or records.
- Do not include more personal or clinical information than is necessary in SMS reminders or administrative messages.
- Clinical advice provided electronically must be documented in the patient record where relevant.
- Email, messaging and portal workflows must include processes for messages requiring clinical review, urgent escalation or follow-up.
- Personal email accounts, consumer file-sharing platforms and unapproved messaging applications must not be used for FCD Health patient information.

11. Telehealth, audio, video, photography and recordings

Telehealth consultations must be conducted using approved processes that protect privacy and confidentiality. Staff should confirm patient identity, location and privacy where relevant and document the consultation in the clinical record.

Audio, video, photography, transcription or recording of a consultation must not occur without appropriate patient knowledge and consent. Where a digital transcription or AI-assisted documentation tool is used, it must be approved by FCD Health and subject to privacy, security, consent and data-governance controls. Clinicians remain responsible for reviewing and validating the final clinical record.

12. Students, registrars, observers and third parties

Patients must be informed when FCD Health introduces a student, registrar, observer, learner, support person or other third party into a consultation where consent is required. Patient consent must be obtained and documented in accordance with the Informed Consent Policy. A patient may decline a learner or observer without affecting their care.

Students and learners must receive privacy and confidentiality orientation before accessing clinical information and must only access records necessary for their supervised activities.

13. Access to and correction of records

Patients may request access to, or correction of, personal information held by FCD Health. Requests must be verified, documented and managed in accordance with applicable law and the patient-facing Privacy Policy.

- Verify the identity and authority of the person making the request.
- Assess whether any lawful limitation or exception applies before release.

- Where access is refused or limited, provide the person with the reason and available complaint or review pathway where required.
- Corrections must preserve the integrity of the clinical record; original entries must not be improperly deleted or obscured.
- Where a requested correction is not made, a patient statement may be associated with the record where appropriate.

14. Transfer, release and continuity of health records

Requests to transfer or release health records must be managed through an approved process that verifies identity, authority, scope of request and destination. FCD Health should use secure transfer methods and record what was released, to whom, when and on what authority.

Original clinical records remain under FCD Health control unless lawfully transferred under an approved arrangement. Where another practice or provider requires information for ongoing care, relevant information should be supplied in a timely and secure manner consistent with consent, legal authority and clinical safety.

15. Data quality, retention and secure disposal

Information must be accurate, complete, current and fit for its clinical, operational and reporting purpose. FCD Health will maintain an approved records-retention schedule reflecting applicable legal, clinical, contractual and governance requirements.

Records must not be destroyed merely because a patient is inactive or has transferred care. When information has reached the approved disposal date and there is no lawful, clinical, investigation, litigation-hold, audit or contractual reason to retain it, disposal must be secure and irreversible. Electronic disposal must use approved deletion or de-identification methods and paper records must be securely destroyed.

16. Third-party providers, cloud services and cross-border disclosure

Before a third-party system or service provider handles FCD Health information, the responsible business owner must ensure proportionate due diligence has been completed. This should include, where relevant:

- privacy and information-security assessment;
- data-hosting and data-location review;
- contractual confidentiality and breach-notification obligations;
- subcontractor and integration risks;
- access controls and authentication;
- data retention, return and deletion arrangements;
- business continuity and vendor exit arrangements;
- cross-border disclosure implications under the APPs.

Material new technologies, high-risk data uses and significant changes to information handling should undergo a privacy impact assessment or equivalent documented privacy-risk review before implementation.

17. Direct marketing, health promotion and patient communications

FCD Health distinguishes clinical recalls, reminders and service communications from marketing. Marketing or promotional communications using personal information must comply with applicable privacy, spam and consent requirements and provide an appropriate opt-out mechanism. Patients must not be disadvantaged in access to clinical care because they decline marketing communications.

18. Privacy incidents and data breaches

Any suspected loss, unauthorised access, unauthorised disclosure, inappropriate record access, misdirected communication, compromised account or other privacy/security incident must be reported immediately through the FCD Health incident and escalation process.
The response must include, as appropriate:

- contain the incident and protect affected systems or information;
- preserve evidence and document the facts;
- assess the type and sensitivity of information involved, the people affected and likely consequences;
- assess whether the incident is an eligible data breach under the Notifiable Data Breaches scheme;
- notify affected individuals and the Office of the Australian Information Commissioner where legally required;
- consider contractual, funding, insurer, cyber, professional, law-enforcement or other notification obligations;
- complete corrective actions, lessons learned and control improvements;
- escalate material incidents through Executive, SQRCG and Board assurance pathways as appropriate.

19. Privacy complaints

Privacy complaints may be made through FCD Health's consumer feedback and complaints channels or directly to the Executive Office. Complaints must be handled respectfully, confidentially and in accordance with the Consumer Complaints and Feedback Policy.
Where a person remains dissatisfied after FCD Health has had an opportunity to respond, they may seek external review or make a complaint to the Office of the Australian Information Commissioner or another body with jurisdiction over the matter.

20. Workforce confidentiality and training

Privacy and confidentiality obligations apply before, during and after employment or engagement. All workforce members must complete privacy, confidentiality and information-security training at induction and refresher training at intervals set by FCD Health. Completion is recorded in PracticeHub or the approved training register.
Privacy or confidentiality breaches may result in remediation, restriction of system access, performance management, contract action, notification to regulators or professional bodies, or other action depending on severity and legal obligations.

21. Roles and responsibilities

Role	Responsibilities
Board	Provides governance oversight of material privacy, cyber and information-management risk and receives assurance by exception or through scheduled reporting.
Chief Executive Officer	Overall executive accountability for privacy compliance, risk, resourcing and external escalation.
Chief Operating Officer	Ensures operational systems, vendors, access processes, training, business continuity and corrective actions support privacy compliance across sites.
Director of Clinical Governance	Provides professional oversight of clinical confidentiality, health-record practice, clinical information sharing and privacy-related clinical risk; supports SQRCG review.
Executive Officer / Privacy contact	Coordinates policy administration, privacy enquiries, access/correction requests, complaints, registers, breach coordination and evidence retention as delegated.

Role	Responsibilities
Managers and service leads	Implement local controls, ensure staff training and appropriate access, address privacy risks and escalate incidents.
IT / technology providers	Implement approved technical controls, access administration, logging, backup, incident support and contractual security obligations.
All workforce members	Protect confidentiality, use only approved systems, access information only for authorised work, verify recipients, complete training and report incidents immediately.

22. Monitoring, audit and continuous improvement

FCD Health will monitor privacy and health-information management through proportionate governance activities, which may include:

- training-compliance monitoring;
- user-access and termination audits;
- clinical-record and consent audits;
- privacy incident and complaint trend review;
- vendor and system reviews;
- data-quality and reporting integrity audits;
- privacy impact assessments for material new systems or information uses;
- SQRCG, Executive and Board assurance reporting where risk or materiality warrants.

Actions identified through audit, complaints, incidents, accreditation or risk review must have an owner, due date and closure evidence.

23. Related documents

- FCD Health Data Governance Policy and Data Governance Framework;
- FCD Health Informed Consent Policy;
- FCD Health Consumer Complaints and Feedback Policy;
- FCD Health Incident and Clinical Incident Management Policy;
- FCD Health Branding and Communications Policy;
- FCD Health Workforce Credentialing and Scope of Practice Policy;
- FCD Health Training, Competency and Capability Policy;
- FCD Health Emergency, Cyclone and Business Continuity Manual;
- FCD Health Information Security / ICT procedures and approved system-access procedures;
- patient-facing FCD Health Privacy Policy / Privacy Notice.

24. Definitions

Term	Definition
Personal information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable.
Health information	Sensitive personal information about an individual's health, disability, wishes about future healthcare, or a health service provided or to be provided.
Patient health record	The clinical and administrative record maintained by FCD Health about a patient and their healthcare interactions.

Term	Definition
Confidentiality	The obligation to prevent unauthorised access to or disclosure of information entrusted to FCD Health.
Privacy incident	An event involving actual or suspected inappropriate collection, access, use, disclosure, loss, modification or handling of personal information.
Data breach	Unauthorised access to, disclosure of, or loss of personal information held by an entity.
Privacy impact assessment	A structured assessment of privacy risks associated with a new or changed project, system, data use or information-handling practice.

25. References

- Privacy Act 1988 (Cth) and Australian Privacy Principles;
- Office of the Australian Information Commissioner - Australian Privacy Principles Guidelines and Notifiable Data Breaches guidance;
- Information Act 2002 (NT), where applicable;
- My Health Records Act 2012 (Cth) and relevant rules;
- RACGP Standards for general practices (5th edition), Criteria C6.3 and C6.4;
- applicable ACHS, Medicare Urgent Care Clinic, professional and contractual requirements.

26. Document control and approval

Version	Published	Effective	Review	Amendment
1.0	14/12/2024	14/12/2024	14/06/2025	Initial Privacy and Confidentiality Policy
1.2	05/01/2026	05/01/2026	05/02/2027	Darwin Medicare UCC added
3.0	24/09/2026	24/09/2026	24/09/2027	Consolidated organisation-wide Privacy, Confidentiality and Health Information Management Policy

Approval	Details
Approval by	Chief Executive Officer, FCD Health
Approval date	24/09/2026