FCD Health CCTV and Security Camera Policy

Document Name	CCTV and Security Camera Policy
Document ID	FCD-SEC-001
Authority	FCD Health Ltd.
Responsible Role	Chief Executive Officer
Operational Lead	Chief Operating Officer
Applies To	All FCD Health sites and CCTV/security camera systems

1. Purpose

FCD Health uses closed-circuit television (CCTV) and security cameras for legitimate safety and security purposes, including protecting patients, workers, visitors, premises and property and supporting investigation of significant incidents.

This policy sets limits on where cameras may be located, who may access footage, how footage may be used or disclosed, and how privacy is protected across all four FCD Health services.

2. Scope

This policy applies to fixed CCTV and security camera systems operated by or on behalf of FCD Health at Palmerston GP Super Clinic, Palmerston Medicare Urgent Care Clinic, Darwin Medicare Urgent Care Clinic and FCD Health GP Clinic.

It does not authorise covert surveillance, staff recording on personal devices, clinical photography or body-worn cameras. Those activities require separate lawful authority and governance.

3. Core rule

SECURITY CAMERA - NOT CLINICAL SURVEILLANCE

CCTV is used for safety and security. Cameras must not be used to intrude on private clinical care, routinely monitor staff performance, or record areas where people reasonably expect privacy.

- Cameras must have a legitimate safety, security or asset-protection purpose.
- Camera placement must be proportionate and privacy-aware.
- CCTV will ordinarily record video only; audio recording is not enabled unless specifically approved following legal/privacy review.
- Access to live or recorded footage is restricted to authorised persons.
- Footage is not part of the patient clinical record unless a relevant extract is lawfully incorporated into an incident or other approved record.
- Any suspected misuse, unauthorised access or disclosure must be reported as a privacy/security incident.

4. Permitted camera locations

CCTV may be used in areas where there is a genuine safety or security need, such as:

- external entrances, exits, car parks and building approaches;
- reception and public waiting areas where placement minimises unnecessary capture of confidential information;
- corridors and common access areas;
- restricted access points, stores or other areas containing valuable equipment or medicines where justified;
- areas identified through a documented security or occupational-violence risk assessment.

5. Prohibited or restricted locations

NO CAMERAS IN PRIVATE CARE AREAS
CCTV must not be installed in toilets, showers, change areas or other areas where a person reasonably expects privacy.

- Consultation and treatment rooms require exceptional justification and specific executive, privacy and legal review before any camera installation.
- Cameras must not be positioned to capture computer screens, clinical notes, payment information or other confidential information unnecessarily.
- Staff rooms or break areas should not be monitored unless a documented safety/security risk clearly justifies it and a less intrusive control is not reasonably available.
- Covert surveillance is not authorised by this policy.

6. Signage and transparency

People entering monitored areas should be made aware that CCTV is operating.

- Appropriate signs should be displayed at main entrances and/or monitored areas.
- Signage should identify FCD Health as the organisation responsible for the system and provide a contact pathway for privacy enquiries where practical.
- The purpose of monitoring should be capable of being explained to patients, workers and visitors.
- CCTV should also be described in FCD Health's privacy information where relevant.

7. Audio recording

Audio recording creates substantially greater privacy and legal risk than ordinary video surveillance.

- FCD Health CCTV systems should operate without audio recording by default.
- Microphones or audio capture must not be activated simply because the equipment has that capability.
- Any proposed audio recording requires a documented purpose, legal/privacy review and CEO approval before activation.
- The Northern Territory Surveillance Devices Act regulates use of listening and optical surveillance devices and must be considered before any audio or private-activity recording is introduced.

8. Access to live CCTV

Live viewing is restricted to people who need access for security, emergency response or authorised operational purposes.

- Routine access may be provided only to approved roles or contracted security providers.
- During Code Black, lockdown or another immediate security incident, CCTV may be used to support the Chief Warden, management, security personnel and Police.
- Live viewing must not be used for curiosity, gossip or routine observation of individual workers.
- Access permissions should be reviewed when roles change or access is no longer required.

9. Access to recorded footage

Recorded footage may be accessed where there is a legitimate purpose, including:

- investigation of violence, aggression, theft, damage or security incidents;
- investigation of a WHS or significant clinical/service incident where the footage is relevant;
- responding to a lawful request from Police, a court, regulator or other authorised body;
- investigation of a serious privacy, fraud, misconduct or access-control concern;
- responding to an individual's lawful privacy/access request.

Requests should be directed to the COO, CEO or authorised delegate. Access must be limited to the footage reasonably required for the purpose.

10. Emergency and aggression incidents

FCD Health's Emergency Manual already uses CCTV as a potential support during Code Black/lockdown responses. This policy governs the privacy and access controls around that use.

- Immediate safety and emergency response take priority.
- If safe, authorised staff/security may monitor footage and relay relevant information to Police or the Chief Warden.
- After a serious incident, relevant footage should be identified promptly so it is not overwritten by normal system cycling.
- Footage may support incident review, staff safety planning and evidence preservation.
- CCTV does not replace duress alarms, de-escalation, staffing or other security controls.

11. Retention

CCTV footage should be kept only for as long as reasonably necessary for the approved security purpose.

- Routine footage may be automatically overwritten according to the approved CCTV system configuration.
- The configured retention period must be documented in the site/system register and reviewed when systems change.
- Footage relevant to an incident, complaint, investigation, legal matter or regulatory request must be preserved before routine overwrite.
- Preserved footage should be retained only for as long as required for the relevant purpose and applicable recordkeeping/legal requirements.

12. Copying, exporting and evidence preservation

- Footage should not be exported or copied unless required for an authorised purpose.
- Any exported footage must be stored securely with access restricted to authorised persons.
- The date, time, camera/location, reason for export, person authorising and person receiving the footage should be recorded.
- Where footage may be evidence, preserve the original file where practicable and avoid unnecessary editing or conversion.
- Copies no longer required should be securely deleted in accordance with the approved recordkeeping process.

13. Disclosure to Police and external parties

CCTV footage may contain personal information and must not be disclosed simply because an external party asks for it.

- Police requests should be verified and documented.
- Where immediate disclosure is necessary to respond to a serious threat or active emergency, only relevant footage/information should be provided.
- Non-urgent requests should be reviewed by the COO/CEO or authorised delegate and, where needed, legal/privacy advice obtained.
- Requests from insurers, lawyers, patients, family members, employers or other third parties require an appropriate lawful basis before disclosure.
- A disclosure log should be maintained for exported or externally provided footage.

14. Access requests from individuals

A person may request access to CCTV footage containing their personal information. Requests are managed under FCD Health privacy processes.

- The request should identify the approximate date, time, location and circumstances to allow footage to be located.

- Access may require consideration of the privacy and safety of other people captured in the footage.
- FCD Health may provide an edited copy, still image, supervised viewing or another form of access where appropriate.
- Any lawful grounds for refusing or limiting access should be documented and communicated through the privacy process.

15. Staff and workplace surveillance

CCTV may incidentally capture workers performing their duties, but this does not make continuous performance monitoring an approved purpose.

- Footage should not be routinely reviewed to measure productivity, attendance or minor performance matters.
- Where footage is relevant to a serious incident, safety matter, misconduct allegation or investigation, it may be reviewed through the applicable process.
- Any investigation using CCTV must observe procedural fairness and relevant workplace/privacy requirements.
- FCD Health should tell workers about the existence and general purpose of workplace CCTV.

16. Privacy and security controls

- CCTV systems must use appropriate passwords, account controls and vendor/security settings.
- Remote access should be limited and protected through approved security controls.
- Footage must not be stored in personal devices, personal cloud accounts or unapproved shared folders.
- System administrator and viewing access should be limited to the minimum number of people required.
- Access logs should be enabled/reviewed where the system supports them.
- Vendor access must be limited to authorised installation, maintenance or incident-support purposes.

17. Camera installation and change control

New cameras or material changes to existing CCTV require approval before installation or reconfiguration.

- Document the security risk/purpose being addressed.
- Confirm the proposed field of view and whether a less intrusive control could achieve the purpose.
- Check for capture of consultation areas, computer screens, neighbouring premises or other unnecessary private activity.
- Confirm signage, retention, system access and vendor arrangements.
- For higher-risk installations, complete a privacy impact/risk assessment and obtain legal advice where appropriate.
- Update the CCTV/site register after installation or change.

18. CCTV site/system register

FCD Health should maintain a simple CCTV register for governance and audit.

Record	Minimum detail
Location	Site and camera/area identifier.
Purpose	Security/safety risk addressed.
Field of view	General area captured and any privacy controls.
Audio	Disabled / approved status.
Retention	Normal system retention/overwrite setting.
Access	Approved roles/users/provider.
Signage	Location/confirmation.
Last review	Date and reviewer.

19. Incident reporting and misuse

- Unauthorised viewing, copying, sharing or deletion of CCTV footage must be reported immediately.
- A lost/exported copy or unauthorised disclosure may constitute a privacy/data breach and must be assessed under the Data Breach Response Plan.
- Intentional misuse may lead to access restriction, disciplinary/contractual action and external notification where required.
- A clinically relevant event shown on CCTV may also require a clinical incident report; the CCTV footage itself does not replace that report.

20. Roles and responsibilities

Role	Responsibilities
Chief Operating Officer	Operational owner of CCTV governance, camera approvals, access, retention and incident preservation.
Chief Executive Officer	Executive accountability and approval for higher-risk surveillance, external disclosure or significant exceptions.
Executive Officer	Supports registers, authorised requests, recordkeeping and privacy coordination as delegated.
Director of Clinical Governance	Advises where CCTV is relevant to patient safety or clinical incident review.
IT / security provider	Maintains system security, access controls, configuration and authorised technical support.
Managers / authorised users	Use CCTV only for approved purposes, protect footage and report misuse or incidents.
All workers	Do not access, copy, photograph or share CCTV footage unless authorised.

21. Review and assurance

- Review camera locations, fields of view, access permissions, signage and retention settings at least annually and when systems change.
- Review CCTV access after significant security incidents or suspected misuse.
- Confirm preserved footage is securely disposed of when no longer required.
- Material privacy, security or governance risks are escalated through Executive and the relevant Board assurance process.

22. Related documents

- FCD Health Privacy, Confidentiality and Health Information Management Policy
- FCD Health Data Governance and Information Management Policy
- FCD Health Data Breach Response Plan
- FCD Health Worker Health, Safety and Wellbeing Policy
- FCD Health Managing Aggression, Violence and Challenging Behaviour Policy
- FCD Health Emergency, Cyclone and Business Continuity Manual
- FCD Health Incident and Clinical Incident Management Policy
- FCD Health Digital Communications and Acceptable Use Policy
- FCD Health Code of Conduct

23. Regulatory framework

This policy is informed by the Privacy Act 1988 (Cth) and Australian Privacy Principles as they apply to private health service providers, and the Surveillance Devices Act 2007 (NT). FCD Health will apply current legal requirements if surveillance or privacy law changes.

24. Definitions

Term	Definition
CCTV	A closed-circuit television or fixed video surveillance system used to observe and/or record a defined area.
Footage	Video images or recordings captured by a CCTV/security camera system.
Private activity	An activity carried on in circumstances that may reasonably be taken to indicate the parties desire it to be observed only by themselves, subject to the Surveillance Devices Act.
Authorised user	A person approved to view or administer CCTV for a legitimate FCD Health purpose.
Preserved footage	Footage intentionally retained beyond normal system overwrite because it is relevant to an incident, request, investigation or legal matter.

25. Policy contact: Executive Officer | Executive Team | exec@fcdhealth.org.au

26. Document control

Version	Published date	Effective date	Review date	Effective to	Amendment(s)
1.0	Previous versions	Previous versions	Superseded	Superseded	Earlier CCTV/security camera arrangements.
2.0	25/09/2026	25/09/2026	25/09/2027	25/09/2028	Four-service consolidation covering placement

27. Approval

Approval by	Bernie Cummins, Chief Executive Officer, FCD Health
Approval date	25/09/2026