Clinic | Pro

ClinicPro Capture: Privacy Impact Assessment Report

This report follows the structure of the Office of the Privacy Commissioner's Privacy Impact Assessment Toolkit report template (privacy.org.nz, 2024 toolkit). This assessment is prepared and maintained by NexWave Solutions Limited as part of its Medtech ALEX integration partnership, and is reviewed as the product evolves. It was last updated in August 2026 following recent feature releases.

Version	1.0
Date	August 2026
Author	NexWave Solutions Limited
Privacy officer	Dr Ryo Eguchi, ryo@clinicpro.co.nz
Framework	Privacy Act 2020 Information Privacy Principles (IPPs); Health Information Privacy Code 2020 (HIPC, incorporating Amendment No 2, in force 1 May 2026); HISO 10029 informing the security assessment
Evidence base	Source code of `clinicpro-medtech` at commits `6ac585d` / `c9cb943` and the live public privacy policy, read directly; Bearer static-analysis and OSV dependency scans (August 2026); a dedicated security audit (August 2026); a live review of the production server host (August 2026)

1. Project summary

ClinicPro Capture is a clinical image capture web application for New Zealand general practices using Medtech Evolution. A clinician opens a patient in Evolution, clicks the ClinicPro icon, and a QR code appears; scanning it with a phone opens a camera flow that commits the photograph directly into that patient's Medtech record via ALEX, Medtech's official integration API. A fallback path lets staff search a patient by NHI, and a patient-link path lets a patient upload photos from home through a time-limited, date-of-birth-gated link. One copy of each image ends up in the practice's Medtech record; ClinicPro keeps none.

Operator: NexWave Solutions Limited (NZBN 9429052227875), a New Zealand company and official Medtech ALEX integration partner, built and operated by Dr Ryo Eguchi, a practising Auckland GP.

Role framework. For patient health information, the practice remains the health agency and NexWave acts as its agent under s 11 of the Privacy Act 2020: information handled only as agent is treated as held by the practice, provided the agent does not use or disclose it for its own purposes. The codebase substantiates that proviso: no secondary use path exists, no analytics touch clinical flows, no information is sold, used for marketing, or used to train AI models. For staff account data, NexWave is the agency in its own right and the general IPPs (not HIPC) apply.

Why this PIA exists (threshold assessment). The product routinely handles health information of identifiable individuals, even though it retains almost none of it; it introduces data paths a practice cannot see from the outside (QR handoff, patient upload links, trans-Tasman hosting); and ClinicPro makes public privacy claims that purchasing decisions rest on. A full vendor PIA is warranted, and this is that document, prepared by the vendor so that any practice can read it, satisfy itself, and reference it.

2. Scope of the PIA

2.1 Scope. In scope: collection, use, storage and disclosure of practitioner/staff data; transient processing of clinical images and patient identifiers across all three capture paths; the audit log; data flows between the phone, Vercel, the Lightsail BFF proxy, Supabase and the ALEX API; the jurisdiction of every hop; and verification of ClinicPro's published privacy claims. Out of scope: patient information held inside Medtech Evolution (governed by the

practice and Medtech Global); patient consent for clinical photography (clinical governance at the practice); Medtech Global's own privacy obligations.

2.2 The process. This PIA was prepared against the OPC's PIA Toolkit with a code-verification standard: every factual statement traces to the actual source code (pinned to a named commit), a named report, or a legal instrument, never to a description of the system. A dedicated security audit (August 2026), automated static-analysis and dependency scans, and a live review of the production host feed the assessment. A detailed internal evidence pack holds every citation at full resolution.

2.3 Who has been consulted.

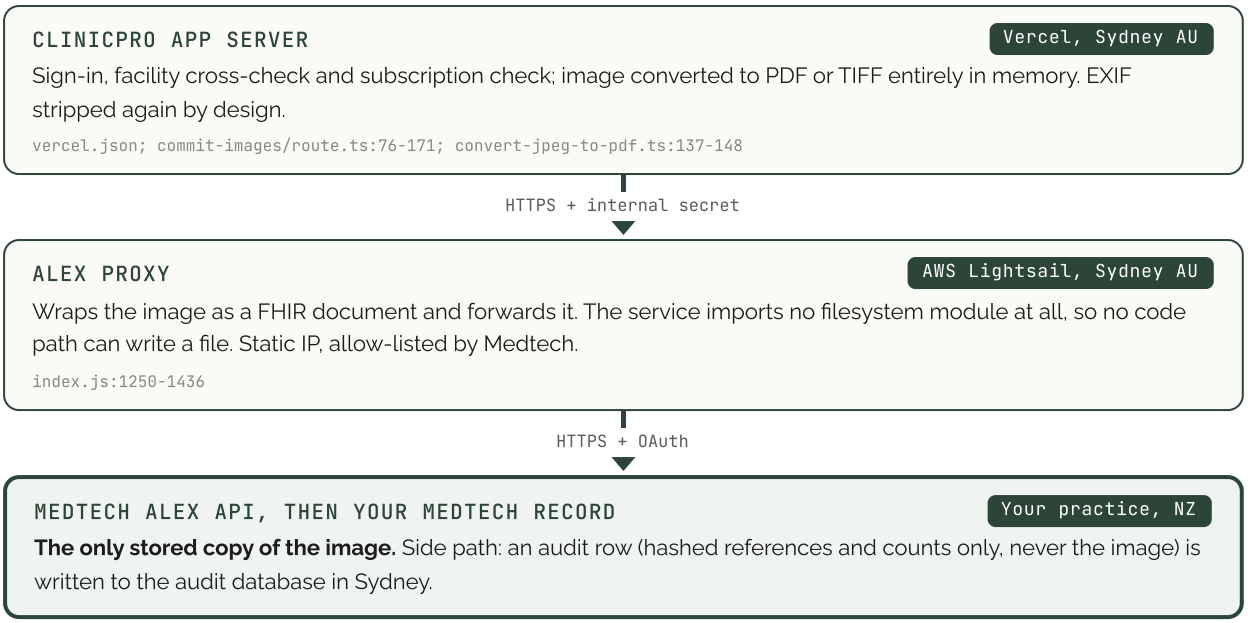
PARTY	STATUS
NexWave / Dr Eguchi (operator, privacy officer)	Involved throughout; all risk-acceptance and position decisions are his
Practices using Capture	A Data Processing Agreement is available to any practice on request
Medtech Global	Deep technical and commercial engagement (consent process, per-facility connection); a written data schedule covering the limited operational data Medtech receives from ClinicPro is being established as an action from this PIA
Infrastructure providers	Standard terms; an AWS NZ Notifiable Data Breach Addendum is in place; a review of Supabase/Vercel support-access statements is in progress

3. Personal information and information flows

3.1 What personal information is involved.

INFORMATION	CATEGORY	WHAT HAPPENS TO IT
Clinical photograph	Health information	Transits in memory only; converted and resized in flight; never written to any ClinicPro database, file store, or log; the only stored copy is the practice's Medtech record
NHI, patient name, date of birth, gender	Health information	Used to find and confirm the right patient against the practice's own record; never stored in readable form by ClinicPro
Audit metadata (who, which facility, which practitioner, when, how many images, Medtech document ID, patient references as one-way keyed hashes)	Health-adjacent metadata	Stored in append-only audit tables for 10 years, matching the Health (Retention of Health Information) Regulations 1996 minimum
Handoff/upload-link records	Operational	Hold a Medtech reference ID (meaningless outside Medtech's systems) for the life of the link; cleared by a scheduled sweep after expiry
Staff account data (work email, practitioner/facility link, sign-in records, billing contact)	Personal information	Held by NexWave as agency; retained for the life of the subscription plus 90 days

3.2 The image flow (all three capture routes converge on it).



3.3 Access, security and jurisdiction. Authentication is by email one-time code (no passwords); tenancy is derived server-side, so one practice can never reach another's data; the database denies all access from the public interface (row-level security with zero policies, grants revoked); audit tables are append-only at the database-trigger level, so history cannot be rewritten even with administrative keys. Every hop is encrypted in transit. Jurisdiction: phone (NZ) -> Vercel functions (Sydney) -> Lightsail proxy (Sydney) -> ALEX (Medtech, AU) -> practice record (NZ); Supabase auth and database are in Sydney (verified two ways: the production site's own code bundle and the database host itself). What rests in Australia is only the hashed audit metadata: images and readable identifiers only transit. Three disclosed nuances: static page assets (never clinical or health information) serve from a global CDN; staff billing and operational email use US-based providers (Stripe, Resend), as the public privacy policy discloses; and when a practice sends a patient an upload link, the invitation email (the patient's email address as held in the practice's own record, the practice name, and an optional staff message the interface warns must contain no clinical detail) is delivered through the same US-based email provider. That invitation deliberately carries no clinical content, no NHI, no date of birth and no name, precisely because the date-of-birth check on the landing page is the identity gate. Clinical images and health information never pass through these providers. ALEX's test and production registries are fully separate, so test environments physically cannot reach real patient data.

3.4 Verification of ClinicPro's published privacy claims. Each public claim was verified against source code, with live checks on the production host (August 2026):

#	PUBLISHED CLAIM	VERDICT
C1	No clinical image is ever stored server-side	**Confirmed.** No disk, database or log write of image bytes anywhere on the path; the BFF cannot write files at all; the Bearer static-analysis scan found no storage sink
C2	No patient identifier stored on ClinicPro servers	**Confirmed.** The database stores patient references only as one-way keyed hashes; server process logs redact identifiers, and log retention is deliberately capped at 30 days. Technical caveats: audit tables store the Medtech document ID, and handoff rows a Medtech reference ID for the life of the link, both meaningless outside Medtech's systems
C3	EXIF metadata, including GPS, stripped automatically	**Confirmed** for photographs: structurally on the phone and by explicit design server-side; patient-uploaded photos go through the same server-side strip. Patient-uploaded PDF documents are validated (type, size, structure, page count) and passed through unchanged, as documents rather than photographs
C4	Every hop stays within New Zealand and Australia	**Confirmed with caveats.** All clinical-data hops physically NZ/AU; disclosed caveats as in 3.3
C5	Built to meet HIPC 2020, Privacy Act 2020 s 11, HISO 10029	**Substantiated as a design-intent claim** by Section 4's principle-by-principle assessment

#	PUBLISHED CLAIM	VERDICT
C6	Full audit trail: practitioner ID, facility ID, timestamp	**Confirmed.** The audit schema records those and more, append-only at the database level

4. Privacy assessment (principle by principle)

HIPC 2020's rules mirror the IPP numbering; rule text is quoted from the OPC's published code (incorporating Amendment No 2) and factsheets. Compliance assessments are ClinicPro's own, recorded by the privacy officer in August 2026, pending external legal review.

#	PRINCIPLE	INFORMATION INVOLVED AND HOW IT IS MANAGED	ASSESSMENT
1	Purpose of collection (HIPC r1)	Minimal, purpose-bound: images (the product's function), NHI only to resolve a patient (stored hashed), email as sole credential, IDs for authorisation and audit; server-side caps reject over-collection. r1 requires collection "for a lawful purpose… and necessary for that purpose"; every field maps to a named function	Complies
2	Source of information (HIPC r2)	Patient information comes from the practice's own Medtech record via ALEX, at the practice's direction, within the s 11 agent framework	Complies
3	Collection notice, direct (HIPC r3)	Patient-facing notice duties sit with the practice (stated in the public policy); staff see the public policy, and a sign-in collection notice is being added	Complies; improvement scheduled
3A	Collection notice, indirect (HIPC r3A, in force 1 May 2026)	Own-patient record access in a consultation is assessed as "use" of held information rather than fresh indirect collection, with the "already aware" exception available if it were collection. The product nonetheless already shows clinicians an in-app notice before NHI search, acceptance recorded per practitioner and versioned	Complies; exceeds the likely minimum
4	Manner of collection (HIPC r4)	Capture at the point of care by the treating clinician; QR carries no patient data and no login grant; patient links are DOB-gated with a 5-strike lock; a confirm screen prevents wrong-patient capture. r4 requires lawful, fair, not unreasonably intrusive means	Complies
5	Storage and security (HIPC r5; HISO 10029 informing)	Zero image retention; keyed, domain-separated hashing; append-only audit tables; database deny-all; TLS 1.2/1.3 with HSTS; secret-gated fail-closed proxy; rate limiting; test/production registry separation; host hardening verified live; dedicated audit + automated scans, findings fixed or dispositioned. r5's service-provider limb ("everything reasonably within the power… to prevent unauthorised use or disclosure") is addressed by the s 11 agent design, the practice-facing DPA and the provider-terms review	Complies
6	Access (HIPC r6)	Patients: their record is held by their practice; ClinicPro cannot identify patients from its own holdings and redirects requests. Staff: documented procedure, 20-working-day statutory clock	Complies
7	Correction (HIPC r7)	As principle 6; corrections via the privacy officer, statement-of-correction offered if declined	Complies
8	Accuracy before use (HIPC r8)	Identity checked against the live practice record plus a human confirm screen; NHI collisions refuse silent attachment; QR-commit practitioner identity derived server-side from Evolution's own launch context, never trusted from the client	Complies
9	Retention (HIPC r9)	Images never retained; server logs capped at 30 days; audit records 10 years per the Health (Retention of Health Information) Regulations 1996 minimum, with a documented review procedure; handoff rows cleared on a scheduled sweep after expiry; staff data life-of-subscription + 90 days	Complies

#	PRINCIPLE	INFORMATION INVOLVED AND HOW IT IS MANAGED	ASSESSMENT
10	Limits on use (HIPC r10)	The only use of patient data is the commit-and-audit function; no secondary use exists in code	Complies
11	Limits on disclosure (HIPC r11)	The only disclosure is into the practice's own record via ALEX, which is the service itself, authorised by the practice's signed consent: within r11's permission and original-purpose limbs. Operational alerts to Medtech carry counts, facility IDs and a non-reversible fragment (being replaced by a correlation ID); a written Medtech data schedule is in progress	Complies; schedule in progress
12	Disclosure outside New Zealand (HIPC r12)	r12 applies to disclosures made "in reliance on Rule 11" to a foreign person or entity. ClinicPro's position: transfer to infrastructure operated as the agency's (or its agent's) own processor, where the provider does not use the information for its own purposes, is use and storage under s 11, not a r11 disclosure, so r12 is not triggered by the Australian hosting; moreover only hashed audit metadata rests in Australia at all. Fallback position: were it treated as disclosure, r12(1)(c) and (f) are satisfied on reasonable grounds (Australia's Privacy Act 1988; provider agreements). The US-incorporation support-access question is disclosed and under review	Complies (position pending external legal review)
13	Unique identifiers (HIPC r13)	ClinicPro assigns no identifier to any patient. r13(5): an agency "does not assign a unique identifier… by simply recording a unique identifier assigned… by another agency for the sole purpose of communicating with that agency about the individual", which is exactly ClinicPro's transient use of the NHI and Medtech reference IDs. Hash-only storage exceeds r13(6)(b)'s risk-minimisation expectation; r13(7) is not engaged, as patients are never asked for their NHI	Complies; substantively not applicable

Summary and conclusion of the assessment. ClinicPro Capture is **designed to meet the Health Information Privacy Code 2020 and the Privacy Act 2020, operating as agent of the practice under s 11, with HISO 10029 informing its security posture. This assessment verified that design directly against the source code and the running production system, and found the published privacy claims substantiated.** This conclusion is the operator's own position, made in good faith on the evidence in this document, and has not yet had external legal review.

5. Risk assessment

Risks were identified from the code verification, the dedicated security audit, the automated scans, and the live host review, then individually assessed and dispositioned by the privacy officer (August 2026). The full risk and mitigation register is maintained internally and reviewed on the schedule below; in summary, by category:

- **Technology.** Server-side controls (zero image retention, hash-only identifiers, deny-all database posture, deliberately capped log retention) are verified in place. A set of hardening improvements identified by the assessment is in active implementation, and dependency advisories not reachable from any request path are accepted with a standing update cadence.
- **Process.** Retention, incident-response and access-request procedures are now documented (previously informal). A written data schedule with Medtech Global covering the limited operational data it receives is being established. Practice onboarding identity checks rest on the signed consent process plus the face-to-face launcher setup each practice completes with ClinicPro, which the privacy officer has assessed as adequate at current scale and will revisit as the practice count grows.
- **People.** Access to production systems is held by the operator alone, key-based only. Session-lifetime hardening for signed-in devices is in implementation.
- **Governance.** All residual risks carry a recorded acceptance with reasoning by the privacy officer; the improvement plan has named owners and target dates, tracked internally.

Review and monitoring. This PIA is reviewed: on any change to infrastructure, hosting region or deployment architecture; on any Supabase/Vercel region or plan change; on any HIPC or Privacy Act amendment; when a new capture path or data field is added; on any suspected privacy breach (which also activates the incident-response runbook); and annually each August, alongside the retention procedure.

Requests, questions or concerns: Dr Ryo Eguchi, privacy officer, ryo@clinicpro.co.nz. A Data Processing Agreement and this PIA's plain-language one-page summary are available to any practice.