MindBridge Whitepaper

Patient intake that feels like care

Version 1.1

Audience: Clinicians, Clinical Partners, and Investors

Region focus: Australia-first pilot

Romone Dunlop
December 2025

Important notices (non-negotiable):

- **Clinical decision support boundaries:** MindBridge is designed to support intake, documentation, and clinician decision-making. It is **not** a diagnostic tool and does not replace clinical judgment.
- **Safety posture:** MindBridge is designed so that risk/urgency cues route to clinician review. This document describes *intended* controls and evaluation plans. Any claims of clinical impact require prospective validation.
- **Privacy and security:** This document describes a security *posture* and control intent. Actual compliance depends on the deployed configuration, vendor controls, and partner governance.
- **Forward-looking statements:** "Planned" capabilities are not guarantees; timelines depend on resourcing, clinical governance, and integration scope.

Contact for pilots and partnerships:
(Romone@mindbridge.health, Founder.)

Contents

1 Executive Summary

1.1 Problem

Mental health services are constrained not only by clinician supply, but by workflow friction: incomplete referrals, duplicated history-taking, slow triage decisions, and documentation overhead. Intake is frequently the bottleneck that delays care and wastes scarce clinician time.

1.2 Solution

MindBridge is an **AI-assisted intake and triage workflow platform** designed to:

1. capture structured patient-reported information via adaptive questionnaires;
2. convert responses into clinician-ready briefs with provenance;
3. surface risk/urgency **review cues** for clinician oversight;
4. export structured outputs aligned with FHIR questionnaire resources;
5. provide role-based dashboards, audit trails, and routing workflows.

1.3 What we claim (and what we do not)

We claim operational intent: improved intake completeness, faster triage, reduced admin load, better visit preparedness.
We do not claim: autonomous triage, diagnosis, or proven clinical outcomes without prospective validation.

1.4 Partnership ask

MindBridge is seeking:

- clinical advisory partners (workflow fit, safety boundaries, evaluation design),
- pilot sites (Australia-first) with governance and measurement,
- investment (engineering hardening, integrations, compliance readiness, multi-site evaluation).

2 The Problem: Intake and Triage Are the Bottleneck

2.1 Common failure pattern

- Referrals arrive incomplete, inconsistent, or unstructured.
- Staff chase missing info (delays, cost, patient frustration).
- Triage happens with partial signals (risk of under/over-prioritisation).
- Patients repeat their story multiple times.
- Clinicians lose time reconstructing history and writing first-visit notes.

2.2 Root causes MindBridge targets

1. **Information quality:** missing, contradictory, or low-signal intake data.
2. **Routing uncertainty:** triage decisions made with weak evidence.
3. **Duplication:** repeated collection of the same story across services.
4. **Documentation burden:** conversion from narrative to clinician-ready structure.

2.3 Operational success metrics (measurable)

- Intake completeness at time of triage review
- Time-to-triage decision
- Admin follow-up rate for missing information
- Clinician prep/documentation time for first visit
- Patient acceptability and clinician trust

3 Product Overview and Workflow

3.1 Core workflow

1. **Patient intake:** adaptive questionnaires + plain language + accessibility.
2. **Synthesis:** clinician brief + structured narrative + provenance.
3. **Review cues:** risk/urgency cues surfaced for clinician review (no autopilot).
4. **Routing:** waitlist/booking/referral/escalation workflows.
5. **Exports:** structured data aligned with FHIR Questionnaire/QuestionnaireResponse.

3.2 Conceptual workflow diagram

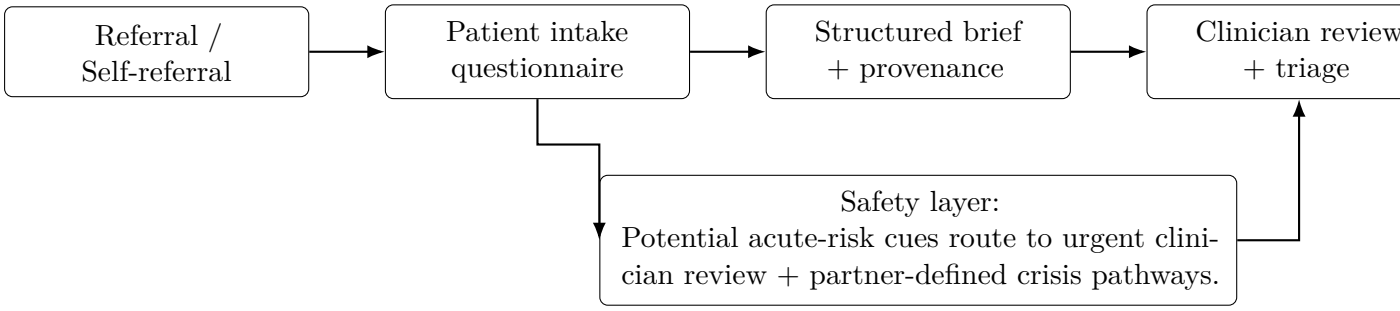

Figure 1: MindBridge intended workflow (conceptual).

4 Interoperability and Structured Data Capture

4.1 Why interoperability is non-negotiable

Mental health care is delivered across systems. If intake outputs are trapped in a single UI, the product creates friction instead of removing it.

4.2 FHIR-aligned approach (high level)

MindBridge is designed to:

- define intake instruments as FHIR `Questionnaire`,
- store responses as `QuestionnaireResponse`,
- export structured payloads where permitted,
- maintain provenance between patient input and derived summaries.

Table 1: Example intake fields to FHIR mapping (illustrative)

Intake element	**FHIR resource**	**Notes (implementation intent)**
Presenting concerns	QuestionnaireResponse.item	Multi-select + free text; stored with provenance
Functional impact	QuestionnaireResponse.item	Work/school, relationships, sleep, self-care
Risk screening items	QuestionnaireResponse.item	Items are *review cues*, not diagnoses
Treatment history	QuestionnaireResponse.item	Meds/therapy history captured as patient-reported
Preferences	QuestionnaireResponse.item	Telehealth preference, accessibility needs
Consent acknowledgements	QuestionnaireResponse.item	Stored explicitly for audit and governance

5 System Architecture (Diligence View)

5.1 Design goals

- **Privacy by design:** least privilege, strong tenant isolation.
- **Auditability:** every derived output traces to source inputs.
- **Safety containment:** AI components cannot take irreversible actions.
- **Integration readiness:** structured outputs designed to travel.
- **Operational resilience:** monitoring + incident response + change control.

5.2 Reference architecture

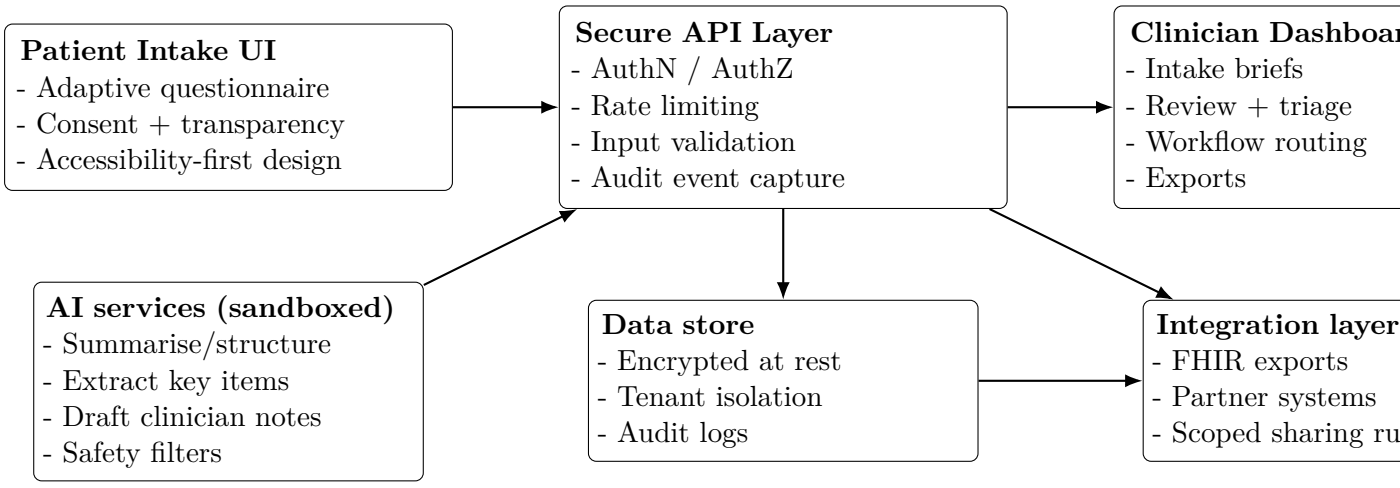

Figure 2: Logical architecture. AI is mediated by governance and cannot silently route safety-critical outcomes.

5.3 Data flow and processing boundaries (diligence-critical)

- **System of record:** define whether MindBridge is the primary store for intake or a transient processor depending on partner requirements.
- **Derived artefacts:** summaries and cues must store provenance and be clearly labelled as derived.
- **Export boundaries:** any export (PDF, FHIR, EHR push) must be explicit, scoped, and logged.

6 Data Governance and Privacy (What Enterprises Ask First)

6.1 Governance objects (what must exist)

A real clinical deployment needs explicit governance artefacts. MindBridge's deployment is designed to support the creation and maintenance of:

- **Data inventory:** what data is collected, why, where stored, retention period.
- **Data classification:** sensitivity categories (mental health data = highest sensitivity).
- **Purpose limitation:** enforce that data is used only for intake/triage/workflow support as agreed.
- **Access governance:** role definitions + approvals + join/leave processes.
- **Data sharing agreements:** explicit rules for external disclosure and exports.

6.2 Data minimisation model

MindBridge's intake design is built around two principles:

1. **Collect what you can justify.**
2. **Delay/avoid what you cannot justify.**

This is implemented via progressive disclosure: only ask deeper questions when earlier responses indicate relevance.

6.3 Data dictionary (minimum viable)

Table 2: Minimum data dictionary (diligence baseline)

Category	Examples	Sensitivity
Identity & contact	Name, DOB, contact method, emergency contact (optional)	High
Presenting concerns	Free text + structured selections	Highest
Risk screening items	Self-harm ideation items, crisis flags (as review cues)	Highest
Clinical history	Patient-reported diagnoses, meds, prior treatment	Highest
Preferences & access	Telehealth preference, accessibility requirements	High
Operational metadata	timestamps, completion state, routing state	Medium
Audit logs	access events, export events, reviewer decisions	High

6.4 Retention and deletion (non-hand-wavy)

For enterprise trust, you must define retention and deletion as policy:

- **Retention rules** (e.g., separate retention for raw intake vs derived summaries vs audit logs).

- **Legal hold** capability (where required by partner governance).
- **Deletion workflows** (patient request pathways where applicable, and partner-specific rules).

Diligence note: do not promise "we delete everything" while also requiring immutable audit logs. You need a defensible balance.

7 Security and Compliance Readiness (Procurement Reality)

7.1 Threat model (plain language)

Mental health intake systems face predictable attack and failure patterns:

- credential theft and account takeover,
- misconfigured access control / tenant isolation failure,
- insecure exports (PDFs emailed around, over-broad sharing),
- insider access without auditability,
- prompt injection attempts to corrupt summaries or extract data,
- vendor/supply-chain risks.

7.2 Security control families (what you will be assessed on)

Table 3: Security controls (diligence view: what to show evidence for)

Control family	Evidence expectations in diligence
Access control	RBAC matrix, MFA posture, admin controls, session expiry, join/leave process
Audit logging	Who accessed what and when; export logs; tamper-resistant retention
Data protection	encryption in transit/at rest; key management approach; secrets handling
Secure SDLC	code reviews, dependency scanning, CI checks, vulnerability process
Monitoring	alerting, incident detection, uptime/latency, anomaly detection
Incident response	runbooks, notification process, post-incident review practice
Change control	release notes, rollback plan, model change management
Vendor risk	third-party inventory, DPAs, minimum security requirements

7.3 Prompt injection and data exfiltration controls

Your intake system will be attacked indirectly (via text fields). MindBridge is designed to implement:

- input sanitisation and adversarial pattern detection,
- strict output schemas (reduce model "freeform" behaviour),
- separation between raw patient text and model instructions,
- no tool access for the model that could exfiltrate data,
- strong logging for unusual prompts and outputs (for investigation).

7.4 SOC 2-style operating model (non-legal, operational)

If you want enterprise deals, your posture must look like an operating system, not a prototype:

- **Policies:** access, incident response, change management, data retention.
- **Evidence:** logs, approvals, tickets, reviews, documented exceptions.
- **Repeatability:** same process every time, not “we did it once”.

8 Clinical Safety Case and Risk Management (The Section That Makes You Credible)

8.1 Safety case structure (what partners expect)

A defensible safety case includes:

1. Intended use and boundaries (what it does / does not do).
2. Hazard analysis (how harm could occur).
3. Risk controls (prevention, detection, response).
4. Residual risk acceptance (who signs off).
5. Post-market monitoring plan (how you detect issues after deployment).

8.2 Hazard analysis (examples)

Table 4: Hazards and controls (illustrative, must be tailored per pilot site)

Hazard	**How harm occurs**	**Controls (intent)**
Missed high-risk cue	System fails to surface concerning statements	Conservative cue thresholds, clinician review gates, monitoring for near-misses
Overconfident summary	Output presents derived claims as facts	Provenance labelling, calibrated language, clinician edit/override
Inappropriate routing	System suggests wrong urgency band or service type	"Suggestion only", mandatory review, documented rationale
Patient distress	Intake wording triggers distress or shame	Plain language testing, progressive disclosure, skip options with explanation
Privacy breach via exports	PDFs shared insecurely or overbroad access	Export scoping, role controls, watermarking, export logs, policy
Bias / inequity	Poorer quality for certain groups	Subgroup evaluation, bias monitoring, human oversight, iterative improvements

8.3 Escalation policy (must be partner-defined)

MindBridge should not hardcode crisis responses. Each partner site must define:

- which cues trigger urgent clinician review,
- coverage expectations (who is on duty and when),
- what patient-facing crisis instructions display,

- what happens if no clinician is available (fallback).

9 Model Risk Management and Evaluation Protocol

9.1 Model risk management (MRM) is mandatory

If you want serious partners, you need an MRM operating model:

- **Model inventory:** which models, which versions, where used.
- **Model card:** intended use, limits, failure modes, evaluation results.
- **Change management:** how model updates are tested, approved, rolled back.
- **Monitoring:** drift, error sampling, subgroup checks, incident capture.

9.2 Evaluation: what you can measure without lying

MindBridge should be evaluated on three layers:

(1) Output quality (offline)

- clinician-rated summary usefulness (rubric)
- factual consistency vs patient inputs (provenance checks)
- readability and structure quality

(2) Workflow outcomes (pilot)

- time-to-triage decision
- admin follow-up rate
- clinician prep time
- intake completion rate

(3) Safety and reliability

- false negative rate for "urgent review" cues (critical)
- false positive rate (noise that burdens clinicians)
- near-miss reporting and root cause analysis

9.3 Clinician rating rubric (example)

9.4 Bias and subgroup evaluation

Minimum diligence requires subgroup checks across:

- age bands, gender identity (where collected ethically), language proficiency,
- neurodiversity/accessibility needs (where relevant),

Table 5: Clinician evaluation rubric (example; customise per partner)

Dimension	**Rating guidance (1–5)**
Usefulness	Does this save time and improve readiness for first contact?
Accuracy vs inputs	Are claims traceable to patient responses without hallucination?
Structure	Clear sections: concerns, history, function, goals, risks, next steps
Safety wording	No diagnosis language; no overconfidence; correct escalation tone
Noise level	Does it include irrelevant detail or miss key information?

- rural vs metro access constraints (workflow differences).

Non-negotiable: if you do not measure subgroup performance, you are blind to inequity.

10 Implementation, Change Management, and Operations

10.1 Pilot implementation plan (90-day practical)

1. **Week 1–2:** scope, governance, risk workshop, baseline measurement plan.
2. **Week 3–4:** intake instrument configuration, routing workflow mapping, role setup.
3. **Week 5–6:** clinician training, dry runs, safety escalation drills.
4. **Week 7–10:** live pilot, weekly review meetings, quality sampling.
5. **Week 11–12:** outcome analysis, safety case update, rollout recommendation.

10.2 RACI (who owns what)

Table 6: RACI matrix (template structure; populate per pilot)

Activity	**Clinic Sponsor**	**Clinical Lead**	**Privacy/Security**	**MindBridge**
Define intended use	A	R	C	R
Configure escalation policy	C	A/R	C	R
Approve intake instrument	C	A/R	C	R
User access / RBAC	C	C	A/R	R
Incident response	C	C	A/R	R
Model updates	C	C	C	A/R
Evaluation reporting	A	R	C	R

10.3 Operational monitoring (minimum baseline)

- uptime and latency SLOs
- error rates (API + client)
- unusual access patterns
- export frequency and destination
- model output sampling + clinician feedback loop

11 Economics and ROI (How Buyers Justify This)

11.1 ROI model (variable-based, not fake numbers)

You should sell MindBridge on **time reclaimed** and **throughput**. Use a simple model:

Table 7: ROI variables (site-specific)

Variable	Definition
N	new intakes per month
T_a	admin minutes saved per intake
T_c	clinician minutes saved per intake (prep/documentation)
C_a	admin cost per hour
C_c	clinician cost per hour
P	monthly platform cost

Estimated monthly value (labour only):

$$Value = N \cdot \left(\frac{T_a}{60} C_a + \frac{T_c}{60} C_c \right) - P$$

Diligence note: do not present this as guaranteed. Use it as a structured justification framework, then validate with pilot measurement.

11.2 Additional value drivers (often bigger than labour)

- fewer missed appointments due to better onboarding,
- reduced referral churn from incomplete information,
- improved routing (right service first time),
- better documentation quality for compliance and continuity of care.

12 Procurement Pack (What to Hand Over in Enterprise Sales)

12.1 What you should provide on day one

- security overview (architecture + controls + data flow)
- data inventory and retention policy
- incident response plan (who/when/how)
- access control model (RBAC roles, MFA posture, audit logging)
- vendor list (subprocessors) and where data is processed
- evaluation plan (metrics, sampling, safety monitoring)
- change management process (including model updates)

12.2 Enterprise questionnaire readiness checklist

Table 8: Enterprise readiness checklist (answer these without guessing)

Question	**You need**
Where is data stored and processed?	Deployment region, vendor inventory, subprocessors
How do you enforce tenant isolation?	Technical mechanism + tests + access controls
How is data encrypted?	In transit and at rest + key management approach
Do you support MFA and SSO?	Current posture + roadmap + admin controls
What audit logs exist?	Access logs, export logs, changes, reviewer actions
How do you handle incidents?	Runbooks + notification timeline + responsibilities
How do you validate model changes?	Test suite, offline eval, sign-off, rollback
How do you manage retention/deletion?	Policy + workflow + audit trail

13 Roadmap (24-month Diligence View)

Table 9: Roadmap (indicative; depends on partner governance and resourcing)

Phase	**Focus**
0–3 months	Pilot hardening: provenance UI, audit completeness, escalation configuration, instrumentation
3–6 months	Clinical advisory loop: rubric evaluation, weekly safety review, workflow optimisation
6–12 months	Integrations: expanded FHIR exports, partner-specific routing workflows, reporting dashboards
12–24 months	Multi-site validation, enterprise governance (SSO, policy packs), procurement readiness

14 Key Risks and Mitigations

Table 10: Risks and mitigations (investor/clinical diligence view)

Risk	**Failure mode**	**Mitigation (intent)**
Safety-critical errors	Missed urgent cues or misleading summaries	Review gates, conservative cues, monitoring, incident response
Clinician distrust	Tool perceived as black box or liability	Provenance, edit/override, auditability, clear boundaries
Privacy breach	Unauthorised access/exfiltration	RBAC, tenant isolation, encryption, logging, testing
Workflow mismatch	Adds steps instead of removing friction	Co-design, pilot iteration, measurable outcomes
Unvalidated claims	Overpromising reduces credibility	Strict claims discipline, evaluation plan, transparent reporting
Integration delays	EHR variability slows deployment	FHIR-first scope, staged integration, narrow pilot

15 Call to Action: Clinical Partners and Investment

15.1 Clinical partners

We are seeking clinician advisors and pilot sites to:

- validate intake structure and safety workflows,
- co-design triage review cues and escalation policies,
- define and measure operational outcomes,
- oversee ethical deployment and patient communication.

15.2 Investors

We are seeking investment to:

- harden the product for clinical deployment,
- fund integrations and governance/compliance readiness,
- support multi-site evaluation,
- build a durable workflow platform with strong defensibility.

A Appendix A: Example Intake Domains (Structure)

Actual question sets must be configured per partner governance and cohort.

1. Identity and contact (minimal required)
2. Presenting concerns (free text + structured selections)
3. Symptoms and severity (structured)
4. Duration and trajectory
5. Functional impact
6. Risk screening cues (partner-defined; review gated)
7. Treatment history (patient-reported)
8. Preferences and access needs
9. Goals (what improvement means to the patient)

B Appendix B: Glossary

- **FHIR:** Fast Healthcare Interoperability Resources.
- **SDC:** Structured Data Capture (FHIR questionnaires).
- **RBAC:** Role-Based Access Control.
- **MRM:** Model Risk Management.
- **Review cue:** signal prompting clinician attention (not a diagnosis).