

Clin- 醫療生態系

從民眾看得懂，到醫事用得動

江家寓 / Chia-Yu Chiang

銘傳大學 生物醫學工程學系 • 2026

我看到的問題

民眾端：拿到體檢報告，一堆數字與術語，不知道哪些該擔心。

- 資訊不對等 • 隱私顧慮（貼到 ChatGPT 不安全）

醫事端：台灣基層診所資訊化落差大。

- 大醫院有 HIS/EMR，中小診所買不起、或流程不合用

Clin- 生態系：一個環環相扣的系統

作品	定位	一句話
ClinCalc （民眾端）	入口	把報告變得 看得懂
ExClinCalc Pro （醫事端）	流程	診所完整工作流，安全做在 資料庫層
clinconvert	標準化（POC）	FHIR 資料轉換概念驗證
Kaizei	跨領域	同套工程方法跨領域複用

共用技術主軸：**Cloudflare Workers + Supabase + PostgreSQL RLS + TypeScript**

作品一：ClinCalc

民眾健康自查 + AI 解讀

ClinCalc 的兩個核心設計

1. 本地優先解讀

- 35 項體檢指標、KDIGO 2024 慢性腎臟病分期
- 判讀邏輯**全在瀏覽器完成**，原始數值不離開裝置

2. AI 為輔、不為主

- 先在本地判定「正常 / 偏高 / 偏低」→ **只把結構化結果**交給 Gemini
- AI 不需記憶正常範圍 → 幻覺率與隱私風險都降低

ClinCalc：先規則後 LLM

使用者填 35 項指標



本地知識庫 `referenceRanges.ts` ← KDIGO 2024 / ADA / ACC-AHA



`checkAbnormal()` 判定：正常 / 偏高 / 偏低 / 嚴重...



只把「結構化判定」組 prompt → Gemini 做整體建議

可追溯：每個判定都對得回來源指引，不是 AI 憑空生成。

作品二：ExClinCalc Pro

診所臨床決策工作站

ExClinCalc：完整診所流程閉環

不是病歷編輯器，是**五個環節環環相扣**：

掛號 → 護理分診 → 醫師 SOAP 七步驟 → 藥物交互檢查 → 藥師調配

- SOAP 依主訴自動展開引導問題
- 開處方即時跳出藥物交互警示
- 六種角色：醫師 / 護理師 / 藥師 / 行政 / 管理員 / 超級管理員

★ 最核心：安全做在資料庫層

醫療資料的權限，我**沒有寫在後端程式裡**，而是下沉到 PostgreSQL。

41 條 Row Level Security policy

就算前端被攻破，攻擊者也拿不到不屬於他角色的資料——
因為 PostgreSQL 在**每一筆查詢前**都先比對身分與權限。

縱深防禦：後端程式一定會有漏洞；把權限放進 DB，是「應用層失守、資料仍安全」。

安全設計的三個深度

- **強制 MFA**：所有醫事人員存取病患資料必過 TOTP 動態碼 (AAL2)
- **RESTRICTIVE 閘門**：用 PostgreSQL 的 restrictive policy 把 MFA 以 **AND** 硬套上 → 任何政策都繞不過
- **角色能力矩陣**：藥師只能配藥不能改診斷、護理師寫的生命徵象只有醫師能讀

以 8 個 migration 建構、40+ 條 RLS 整合測試驗證。

怎麼驗證安全沒寫錯？

在一次性的 Postgres 上，**模擬各角色的 session**，直接測 RLS：

情境	預期	結果
醫師 無 MFA(aal1)	拒絕 PHI	✓
醫師 有 MFA(aal2)	放行 PHI	✓
藥師 竄改診斷	被 trigger 擋	✓
匿名存取	拒絕	✓

安全不靠嘴說，靠測試證明。

技術棧與部署

- **前端**：Next.js 16 (App Router) • React 19 • TypeScript • Tailwind v4
- **後端 / DB**：Supabase (PostgreSQL + Auth + RLS + TOTP MFA)
- **AI**：Google Gemini (先規則後 LLM)
- **部署**：Cloudflare Workers (OpenNext)，全球邊緣節點，成本極低

兩端**共用同一份 Supabase**，靠 RLS 隔離：

民眾只看自己的記錄，醫師需**一次性同意書授權**才能查閱。

我學到什麼 / 想延伸的研究

1. 多租戶醫療系統的 RLS 設計方法論

能不能從業務需求**自動推導**權限規則、再**形式化驗證**其完整性？

2. LLM 安全嵌入臨床流程的分級架構

「先規則後 LLM」怎麼分配介入比例、怎麼量化評估幻覺與覆蓋率？

3. CDSS 的真實場域評估方法

從「功能完整」到「實際導入」——使用者接受度、警示疲勞怎麼量測？

謝謝

江家寓 • yuyulsc881209@icloud.com

線上 Demo : clincalc / exclincalc `.yuyulsc881209.workers.dev`

GitHub : github.com/yu8812 • 個人網站 : jiayuselfweb.pages.dev