THERMOEYE PLANNING DOCUMENT

สรุประบบ Thermoeye และแผนระบบหลังบ้าน

เอกสารสรุปสิ่งที่จะสร้าง: ระบบรับข้อมูล OCTA/OCT จากโรงพยาบาลอย่างปลอดภัย ตรวจคุณภาพภาพ วิเคราะห์ด้วย AI แบบตรวจสอบย้อนกลับได้ และสร้างผลคัดกรองที่แพทย์อ่านง่าย

Product Direction	MVP Strategy	Prepared Date
Secure clinical screening workflow	**ระบบจริง + AI mock/baseline ก่อนเสียบโมเดลจริง**	**24 May 2026**

01 / EXECUTIVE SUMMARY

แนวคิดหลักของระบบ

Thermoeye ไม่ควรถูกวางเป็นแค่ “AI ทำนายโรค” แต่ควรเป็น data-to-screening workflow ที่รับข้อมูลจากโรงพยาบาลอย่างปลอดภัย แปลงข้อมูลเป็นผลคัดกรองที่อ่านง่าย และมีหลักฐานย้อนกลับได้ทุกขั้นตอน

> **ข้อกำหนดสำคัญ:** ระบบเวอร์ชันแรกควรวางตัวเป็น clinical decision support สำหรับการคัดกรองความเสี่ยง ไม่ใช่เครื่องมือวินิจฉัยโรคแทนแพทย์ ผลลัพธ์ต้องผ่านการ review/approve โดยแพทย์ก่อนใช้งานจริง

เป้าหมายระบบ

- รับภาพ OCTA/OCT และข้อมูลผู้ป่วยที่จำเป็นจากโรงพยาบาลหรือคลินิกพาร์ทเนอร์
- ปกป้องข้อมูลผู้ป่วยด้วย de-identification, consent tracking, access control และ audit log
- ตรวจคุณภาพภาพก่อนส่งเข้า AI เพื่อลดความเสี่ยงจากผลวิเคราะห์ที่ผิดพลาด
- วิเคราะห์ vessel/capillary density และแปลงเป็น risk score: Low, Moderate, High
- แสดงผลแบบ explainable ด้วย heatmap, segmentation และคำอธิบายที่แพทย์อ่านง่าย
- สร้าง PDF report และ dashboard สำหรับโรงพยาบาล
- เก็บ feedback จากแพทย์เพื่อพัฒนาโมเดลใน training sandbox ที่ควบคุมได้

ขอบเขตที่ควรทำก่อน

ขอบเขต	สิ่งที่จะทำใน MVP	สิ่งที่ต้องใช้ข้อมูลจริงภายหลัง
ระบบเว็บและ workflow	ทำได้ครบ: login, upload, case, dashboard, report, audit	ปรับตาม workflow จริงของโรงพยาบาล
AI วิเคราะห์ภาพ	ใช้ mock/baseline engine และโครง service ที่ต่อโมเดลจริงได้	ต้องมี OCTA dataset, label, ground truth และ clinical validation
Regulatory	วางเอกสาร intended use, risk log, model version, audit trail	ต้องทำ validation, quality management และขออนุมัติกับหน่วยงานที่เกี่ยวข้อง

02 / PRODUCT SCOPE

ฟีเจอร์หลักที่จะสร้าง

Hospital Data Ingestion

รับข้อมูลจากโรงพยาบาลผ่าน portal, API หรือไฟล์มาตรฐาน เช่น OCTA/OCT image, scan metadata, case ID, age, sex และวันที่ตรวจ

Privacy Protection

ลบข้อมูลระบุตัวตนโดยตรง ใช้ case code แทนตัวจริง แยก mapping table และเก็บ raw data ในพื้นที่จำกัดสิทธิ์

Image Quality Check

ตรวจ blur, missing frame, artifact, format, resolution และ macula region ก่อนส่งเข้า AI หากภาพใช้ไม่ได้ต้องแจ้งให้ scan ใหม่

AI Analysis Engine

เตรียม pipeline สำหรับ preprocessing, segmentation, vessel density calculation, risk score และ confidence score

Explainable Output

แสดง original image, segmentation, heatmap, vessel density และเหตุผลสั้น ๆ ที่ทำให้แพทย์ตรวจสอบผลได้

Report Generator

สร้างรายงาน PDF สรุป risk level, key metrics, recommendation, model version และสถานะการ review โดยแพทย์

Partner Dashboard

แสดงจำนวนเคสที่ส่งมา เคสเสี่ยงสูง trend รายเดือน ประสิทธิภาพระบบ และประวัติการตรวจย้อนหลัง

Feedback Loop

เก็บผลยืนยันจากแพทย์ ผลติดตามซ้ำ และ label correction เพื่อส่งเข้า curated dataset ก่อนใช้ train โมเดลใหม่

ฟีเจอร์กำกับความปลอดภัย

- Role-Based Access Control
- Audit Log
- Consent Tracking
- Data Agreement Layer
- Secure Storage
- Model Registry
- Training Sandbox
- Retention Policy

> จุดขายของระบบไม่ใช่แค่โมเดล AI แต่คือ workflow ที่ทำให้โรงพยาบาลรับข้อมูล วิเคราะห์ ตรวจสอบผล ออกรายงาน และย้อนกลับไปพัฒนาโมเดลได้อย่างเป็นระบบ

03 / WORKFLOW

ลำดับการทำงานที่เหมาะสม

1. **Hospital Upload / API Ingestion**
   โรงพยาบาลส่งภาพ OCTA/OCT พร้อมข้อมูลที่จำเป็นเท่านั้น เช่น case ID, อายุ, เพศ, scan type และวันที่ตรวจ

2. **Raw Quarantine Storage**
   เก็บไฟล์ต้นฉบับในพื้นที่เข้ารหัสและจำกัดสิทธิ์ เพราะ raw file อาจมีข้อมูลระบุตัวตนใน metadata หรือบนภาพ

3. **Consent & Data Agreement Check**
   ตรวจว่าข้อมูลนี้ใช้ได้เพื่ออะไร: screening, research, model development หรือ follow-up

4. **De-identification**
   ลบชื่อ เลขบัตร ประวัติระบุตัวตน และแปลงเป็น case code โดยแยก mapping table ไว้ในสิทธิ์ที่เข้มงวด

5. **Image Quality Check**
   ตรวจคุณภาพภาพก่อนเข้า AI หากภาพไม่ผ่านให้แจ้งเหตุผลและแนะนำให้ scan ใหม่

6. **AI Analysis**
   ประมวลผลภาพ คำนวณ vessel/capillary density และสรุปเป็น risk score พร้อม confidence

7. **Explainable Result**
   แสดง heatmap, segmentation, key metrics และคำอธิบายที่แพทย์ตรวจสอบได้

8. **Doctor Review & Report Release**
   แพทย์ review/approve ผลก่อนปล่อยรายงานให้โรงพยาบาลหรือคนไข้

9. **Feedback to Model Improvement**
   เก็บผลยืนยันจริงและ follow-up เข้า curated dataset ก่อนนำไป train/validate โมเดลเวอร์ชันใหม่

> ลำดับสำคัญ: de-identification ควรเกิดก่อน pipeline ปกติ และ feedback loop ไม่ควร auto-train จาก

> production โดยตรง ทุกโมเดลใหม่ต้องผ่าน validation, bias check และ release approval ก่อนใช้งาน

04 / BACKEND ARCHITECTURE

ระบบหลังบ้านที่ต้องมี

Module / Service	หน้าที่	ข้อมูลสำคัญ
Auth & RBAC	จัดการ login, session, role, permission และ multi-tenant hospital access	user, role, hospital, permission
Case Management	จัดการผู้ป่วยแบบจำกัดข้อมูล เคสตรวจ สถานะ workflow และ doctor review	case, scan, review, status
Ingestion API	รับไฟล์จาก portal, API หรือ DICOM/FHIR gateway ใน phase ถัดไป	upload record, metadata, source
De-identification Service	ลบ PHI/PII จาก metadata และจัดการ pseudonymous case code	de-id log, mapping reference
Storage Service	แยก raw, processed, report และ training dataset พร้อม encryption policy	object key, checksum, retention
Quality Check Worker	ตรวจ blur, artifact, format, resolution และ scan validity ก่อนเข้า AI	quality status, reason, score
AI Analysis Worker	วิเคราะห์ภาพแบบ async ผ่าน queue เพื่อไม่ให้เว็บค้าง	risk score, confidence, metrics
Explainability Service	สร้าง heatmap, segmentation overlay และ feature summary	overlay image, vessel density
Report Service	สร้าง PDF report พร้อม model version และ review signature	report file, release status
Audit Log Service	บันทึกว่าใครดู แก้ อัปโหลด ดาวน์โหลด หรือ approve อะไร	actor, action, target, timestamp
Model Registry	ควบคุม model version, threshold version, training dataset version และ release gate	model, metric, deployment
Analytics Dashboard	สรุปจำนวนเคส trend ความเสี่ยง ประสิทธิภาพระบบ และข้อมูลเชิงบริหาร	aggregate metrics

สถานะเคสที่ควรใช้

received | de_identified | quality_checked | analysis_running | ai_completed | doctor_reviewed | report_released | feedback_received

05 / TECHNOLOGY STACK

เทคโนโลยีที่แนะนำให้ใช้

Layer	แนะนำ	เหตุผล
Frontend	Next.js + React + TypeScript	เหมาะกับ dashboard, portal, role-based UI, PDF preview และ deploy ง่าย
Backend API	FastAPI + Python	ต่อกับ AI/image processing ได้ง่าย ทำ REST API เร็ว และรองรับ async workflow
Database	PostgreSQL	เหมาะกับข้อมูลเชิงธุรกรรม เคส ผู้ใช้ consent audit และ reporting
Object Storage	S3-compatible storage / MinIO สำหรับ local dev	เหมาะกับไฟล์ภาพ medical image, processed image, heatmap และ PDF report
Queue & Worker	Redis + Celery หรือ RQ	ใช้รัน quality check, AI analysis และ report generation แบบ background job
Image Processing	OpenCV, Pillow, scikit-image	เริ่มจาก rule-based quality check และ image preprocessing ได้ทันที
AI / ML	PyTorch หรือ TensorFlow	รองรับ segmentation model, classification model และ experiment ต่อในอนาคต
Report	HTML-to-PDF หรือ server-side PDF generation	ควบคุม layout รายงานแพทย์ได้ดี และแนบผลภาพ/metrics ได้
Observability	Structured logs, metrics, error tracking	ใช้ตรวจสอบงาน background, security event, pipeline failure และ model drift
Deployment	Docker Compose สำหรับ dev, cloud/container สำหรับ production	แยก service ชัดเจนและ deploy ซ้ำได้ง่าย

มาตรฐานที่ควรรองรับใน phase ถัดไป

- **DICOM / DICOMweb:** สำหรับเชื่อมต่อข้อมูลภาพทางการแพทย์จากระบบ imaging หรือ PACS
- **HL7 FHIR:** สำหรับข้อมูลผู้ป่วย เคสตรวจ และข้อมูลสุขภาพที่ต้องแลกเปลี่ยนกับโรงพยาบาล
- **SaMD documentation:** intended use, risk management, validation, change control และ model release record
- **PDPA-ready data governance:** consent, purpose limitation, data minimization, retention และ deletion request

06 / DATA MODEL

ฐานข้อมูลหลักที่ควรมี

Entity	ตัวอย่างข้อมูล	หมายเหตุด้านความปลอดภัย
Hospital	name, code, contact, subscription plan	ใช้แยก tenant และสิทธิ์การเข้าถึง
User	name, email, role, hospital_id, status	ต้องมี MFA ใน production และ session policy ชัดเจน
Case	case_code, age, sex, scan date, status	ไม่ควรเก็บข้อมูลระบุตัวตนเกินจำเป็น
Consent	screening allowed, research allowed, model training allowed, expiry	ต้องตรวจทุกครั้งก่อนใช้ข้อมูลนอกวัตถุประสงค์เดิม
Scan	scan type, eye side, device, image object key, checksum	ไฟล์ภาพต้องเก็บใน object storage แบบเข้ารหัส
Quality Check	pass/fail, blur score, artifact score, failure reason	ถ้า fail ต้องหยุดก่อนเข้า AI analysis
Analysis Result	risk score, risk level, confidence, vessel density, model version	ต้องผูกกับ model และ threshold version เสมอ
Review	doctor decision, note, approved_at, reviewer_id	ผลใช้งานจริงควรมี human approval
Report	report number, PDF object key, release status	download ต้องถูก log ทุกครั้ง
Feedback	confirmed diagnosis, follow-up result, correction, label status	ต้องเข้า curated dataset ก่อนใช้ train model
Audit Log	actor, action, target, IP, timestamp	ควร append-only และค้นย้อนหลังได้

> หลักการฐานข้อมูล: แยกข้อมูลระบุตัวตน ข้อมูลเคส ข้อมูลภาพ และข้อมูลสำหรับ training ออกจากกัน ลดการเข้าถึงข้ามส่วน และทำให้ลบ/จำกัดการใช้งานข้อมูลได้ตาม consent

07 / SECURITY & GOVERNANCE

ข้อกำหนดด้านความปลอดภัยและข้อมูลผู้ป่วย

Access Control

- แยก role: admin, hospital staff, doctor, researcher
- จำกัดข้อมูลตาม hospital/tenant
- ใช้ least privilege เป็นค่าเริ่มต้น

Audit Trail

- log การดูข้อมูล อัปโหลด ดาวน์โหลด แก้ไข และ approve
- เก็บ actor, target, action, timestamp และ IP
- ใช้ตรวจสอบเหตุการณ์ย้อนหลังได้

Data Protection

- encrypt at rest และ encrypt in transit
- แยก raw, processed, report, training dataset
- กำหนด retention และ deletion policy

Consent & Agreement

- เก็บ purpose ของข้อมูลแต่ละเคส
- แยกสิทธิ์ screening, research, model development
- ระบุว่า hospital เป็นเจ้าของข้อมูล และ platform เป็นผู้ประมวลผล

ความเสี่ยงที่ต้องควบคุม

Risk	แนวทางควบคุม
ข้อมูลผู้ป่วยรั่วไหล	de-identification, encryption, RBAC, audit log, secret management และ incident response plan
AI วิเคราะห์ผิดจากภาพคุณภาพต่ำ	quality gate ก่อนเข้า AI และแสดงเหตุผลเมื่อภาพไม่ผ่าน
โมเดล bias กับบางกลุ่มหรือบางเครื่อง scan	monitor ตาม hospital, scanner, age group, sex และ image quality
ใช้ข้อมูลเกิน consent	purpose check ก่อน export/research/training และบันทึก audit ทุกครั้ง
เปลี่ยนโมเดลแล้วผลย้อนหลังอธิบายไม่ได้	model registry, threshold version, release note และ immutable analysis record

08 / DELIVERY PLAN

แผนการพัฒนาเป็น Phase

Phase	เป้าหมาย	Deliverables
Phase 1: MVP Workflow	ทำระบบที่ใช้งาน end-to-end ได้ด้วย mock/baseline AI	login, hospital dashboard, case, upload, de-id, quality check, mock analysis, report, audit
Phase 2: Clinical Pilot Readiness	เตรียมระบบสำหรับทดลองกับโรงพยาบาลพาร์ทเนอร์	consent, data agreement, API ingestion, stronger security, doctor review, feedback module
Phase 3: Real AI Integration	เริ่มใช้โมเดล segmentation/risk model จากข้อมูลจริง	model registry, validation dashboard, bias/drift monitoring, training sandbox
Phase 4: Hospital Integration	เชื่อมระบบโรงพยาบาลจริง	DICOMweb/PACS integration, FHIR/API mapping, production deployment, operational monitoring
Phase 5: Regulatory & Scale	เตรียมขยายเชิงพาณิชย์และ regulatory	clinical validation package, quality process, SaMD documentation, certification preparation

คำแนะนำแบบ senior

- อย่าเริ่มจาก AI ก่อน ให้เริ่มจาก secure workflow และ data governance ก่อน เพราะเป็นสิ่งที่โรงพยาบาลต้องเชื่อถือ
- ทำ mock AI ให้หน้าระบบและ pipeline เหมือนของจริง เพื่อให้เปลี่ยนเป็นโมเดลจริงภายหลังได้โดยไม่รื้อระบบ
- ทุกผลวิเคราะห์ต้องบอกได้ว่าใช้ข้อมูลอะไร โมเดลเวอร์ชันไหน threshold ไหน และใครเป็นคน approve
- การใช้ข้อมูลโรงพยาบาลเพื่อ train model ต้องผ่าน consent, curation, validation และ release gate ไม่ใช่เอา production data ไป train อัตโนมัติ

เอกสารนี้เป็น technical/product planning summary สำหรับเริ่มพัฒนา prototype และ MVP ไม่ใช่เอกสารรับรองผลทางการแพทย์หรือเอกสาร regulatory ฉบับสมบูรณ์