RALPHGUARD

การพัฒนา OCR และ AI Assistant

สรุปสถาปัตยกรรม กระบวนการตรวจสอบ และแนวทางใช้งานอย่างรับผิดชอบ

OCR หลายรอบ

ทะเบียนสาร 1,336 รายการ

AI พร้อมเสียง

เอกสารฉบับพัฒนา | 24 กรกฎาคม 2026

ภาพรวมระบบ

RalphGuard แยกปัญหา การรู้จักส่วนผสม ออกจาก การทำนายพิษ ชื่อที่อ่านได้ทุกตัวต้องคงอยู่ในผลลัพธ์ แม้ไม่มีโครงสร้างโมเลกุลเดียวหรือยังไม่เหมาะกับ QSAR

ภาพฉลาก → **OCR + consensus** → **Entity linking** → **QSAR / fallback** → **ผลโปร่งใส**

ส่วน	หน้าที่
OCR	แปลงฉลากเป็นรายชื่อ INCI ด้วย 3 image variants x 3 PSM และ consensus
Ingredient registry	เชื่อมชื่อ, synonym, CAS, PubChem CID, SMILES และ InChIKey พร้อม provenance
QSAR gate	รับเฉพาะโครงสร้างโมเลกุลที่ตรวจแล้วและ qsar_eligible=true
AI Assistant	ตอบจากบริบทสูตร/ผลปัจจุบัน พร้อม action schema และ preview-confirm
Speech	รับเสียงด้วย Web Speech API และตอบด้วย Edge Neural TTS พร้อม browser fallback

หลักการสำคัญ

ระบบห้ามสร้าง SMILES หรือ toxicity label ขึ้นเอง และห้ามทำส่วนผสมที่ประเมินไม่ได้หายไป สารทุกตัวต้องแสดงสถานะ recognized, resolved, qsar_eligible, assessment method และเหตุผลเมื่อ unresolved.

ผลลัพธ์ในเวอร์ชันนี้

- ทะเบียนสาร offline seed 1,336 รายการ: เข้า QSAR 1,329 และรู้จักแต่ไม่เข้า QSAR 7 รายการ
- หน้าประเมินและ Node graph ดึง registry แบบแบ่งหน้า แทนการหยุดอยู่ที่คลังคงที่ 53 สาร
- เครื่อง Clone ใหม่สร้างข้อมูลชุดเดียวกันผ่าน Alembic migration โดยไม่พึ่ง Docker volume เครื่องเดิม

OCR: จากภาพฉลากสู่รายชื่อส่วนผสม

กระบวนการออกแบบให้ตรวจสอบซ้ำได้และลด false positive จากภาพที่มีแสง เงา ความโค้ง หรือ comma หาย

ขั้นตอน	การทำงาน
1. Validate	ตรวจชนิดไฟล์ ขนาด จำนวนพิกเซล และหมุนตาม EXIF
2. Deskew	ทดลองมุม -6 ถึง +6 องศา ช่วง 0.5 องศา เลือกแนวข้อความดีที่สุด
3. Normalize	grayscale และปรับความกว้างเป้าหมายประมาณ 2,200 px จำกัด upscale 4 เท่า
4. Variants	Autocontrast, sharpened และ binary Otsu
5. OCR passes	Tesseract PSM 4, 6, 11 รวมสูงสุด 9 รอบ พร้อม timeout ต่อรอบ
6. Consensus	ให้คะแนนผล อ่านซ้ำระดับชื่อเต็ม และบังคับ approximate match ให้มีอย่างน้อย 2 votes

การเชื่อมชื่ออย่างระมัดระวัง

- ตัดข้อความหลัง Ingredients จนถึง section boundary เช่น warning, address, lot และ marketing
- รองรับช่องว่าง/comma หายด้วย phrase recovery แต่เปรียบเทียบชื่อ INCI เต็ม ไม่จับคำทั่วไปเดี่ยว ๆ
- threshold ของ fuzzy matching เปลี่ยนตามความยาวชื่อ สารชื่อสั้นต้องเข้มงวดกว่า
- raw PubChem candidate ไม่ถูกส่งเข้า QSAR อัตโนมัติ ต้องผ่าน verification และ structure checks ก่อน

OCR confidence แปลว่าอะไร

เป็นตัวชี้วัดคุณภาพการอ่านข้อความ ไม่ใช่ความน่าจะเป็นว่ารายชื่อทุกตัวถูกต้อง ผู้ใช้ต้องตรวจรายชื่อและความเข้มข้นก่อนยืนยัน

Ingredient recognition ไม่เท่ากับ QSAR eligibility

หลัง OCR ระบบจัดสถานะสารเป็นลำดับ แทนการกรองรายการไม่มี SMILES ทิ้งก่อนแสดงผล

Recognized → **Resolved** → **Structure valid** → **QSAR eligible** → **Assessment**

ประเภท	QSAR	หลักปฏิบัติ
Single substance	อาจเข้า QSAR	ต้องมี canonical SMILES ที่ผ่าน RDKit และ provenance
Salt / inorganic	พิจารณาเป็นรายกรณี	ต้องสอดคล้องกับขอบเขต descriptor และโมเดล
Polymer / silicone	มักไม่เข้า	ใช้ knowledge base หรือแสดงข้อจำกัด
Botanical / mixture / fragrance	ไม่แทนด้วยโมเลกุลเดียว	ใช้ fallback, read-across หรือ unresolved
Unknown composition	ไม่เข้า	คงชื่อและเหตุผลไว้ใน formula coverage

ข้อมูลที่ส่งกลับเพื่อความโปร่งใส

- raw OCR text, parsed/normalized ingredient, match candidates และ match confidence
- structure availability, QSAR eligibility, assessment method และ unresolved reason
- summary: total, recognized, structure-resolved, QSAR-assessable, knowledge-base-assessed, unresolved และ coverage

บทบาทของ PubChem

PubChem ช่วยยืนยัน identity, synonym และ structure แต่ไม่ใช่ toxicity training label โดยอัตโนมัติ ข้อมูลที่นำเข้า offline ต้องผ่านตัวกรองและ verification ก่อน

AI Assistant: รับคำสั่ง ตอบ และแก้ workspace อย่างควบคุม

เสียง/ข้อความ → Context → Groq → Guardrails → Preview + Confirm

ชั้น	รายละเอียด
Input	ข้อความหรือ Web Speech API เมื่อเบราว์เซอร์รองรับ
Grounding	ชื่อสูตร ส่วนผสม ความเข้มข้น คะแนน 4 ด้าน confidence, domain และ coverage
Generation	Groq OpenAI-compatible Chat Completions; API key อยู่ฝั่ง Backend
Actions	schema จำกัด: create/set/replace/remove/rename/goto/run/clear
Mutation safety	Frontend แสดงรายการเปลี่ยนแปลงและรอการยืนยันก่อนแก้ workspace
Voice output	Edge Neural TTS ภาษาไทย; browser speechSynthesis เป็น fallback

Scientific guardrails

- ห้ามรับรองสูตรว่าปลอดภัยก่อน Run และห้ามอ้างคะแนนที่ไม่มีใน context
- ห้ามสร้าง SMILES สำหรับสารสกัด/สารผสม และตรวจ action ที่ LLM สร้างก่อนส่งให้ UI
- คำขอสูตรทดสอบคะแนนสูงใช้ reviewed fixture แทนการเดาความเข้มข้นจากชื่อสาร
- confidence ต่ำหรือ out-of-domain ต้องแสดงข้อจำกัดก่อนสรุป

ไม่ใช่การ fine-tune

AI Assistant ปัจจุบันเป็น context-grounded assistant ที่ควบคุมด้วย system prompt และกฎเชิงโปรแกรม
ไม่ได้ฝึกโมเดลใหม่จากบทสนทนาของผู้ใช้

การทดสอบและความพร้อมสำหรับเครื่อง Clone ใหม่

เกณฑ์ส่งมอบใช้ทั้ง automated tests, fresh database migration และ browser smoke test

ขอบเขต	สิ่งที่ตรวจ
Frontend	TypeScript type-check และ Next.js production build
Backend	API, OCR, registry, PubChem evidence และ smoke tests
Scientific	worker tests และ model artifacts ครบ skin, eye, sens, acute
Fresh database	Alembic upgrade บนฐานข้อมูลใหม่ และ registry seed อย่างน้อย 1,000 แถว
Runtime	CORS/API health, assessment queue, chat, TTS, CSS และ WebGL
Repository	verify-clone-ready ตรวจไฟล์สำคัญว่ามีอยู่และถูก track ใน Git

วิธีเริ่มระบบหลัง Clone

- คัดลอก `.env.example` เป็น `.env` แล้วใส่ `GROQ_API_KEY` เฉพาะในเครื่องหรือ deploy secret
- รัน `docker compose up --build` สำหรับ PostgreSQL, Redis, Backend และ Scientific worker
- เปิด terminal ใหม่: `cd frontend`, `npm ci`, `npm run dev`
- รัน `powershell -ExecutionPolicy Bypass -File scripts/verify-clone-ready.ps1` เพื่อตรวจ assets และ models

ความลับและความปลอดภัย

ห้ามใส่ GROQ_API_KEY จริงใน Git, `.env.example`, screenshot หรือเอกสาร PDF ให้ใช้ secret manager ของแพลตฟอร์มเมื่อ deploy

ข้อจำกัดและไฟล์อ้างอิง

RalphGuard เป็นระบบคัดกรอง in-silico ผลไม่ได้ทดแทนการทดสอบมาตรฐาน การประเมินความปลอดภัยโดยผู้เชี่ยวชาญ หรือการวินิจฉัยทางการแพทย์

ข้อจำกัดที่ต้องสื่อสาร

- พอลิเมอร์ สารสกัด น้ำหอม สารผสม และ UVCB อาจไม่มีโครงสร้างเดียวสำหรับ QSAR
- ภาพ 3D เป็นการสื่อสารคะแนน ไม่ใช่การจำลองอาการทางคลินิก
- คุณภาพ OCR ขึ้นกับความคมชัด มุม แสง และความครบของช่วง Ingredients
- คำสั่งเสียงขึ้นกับการรองรับ Web Speech API และสิทธิ์ไมโครโฟนของเบราว์เซอร์
- บริการ Groq และ Edge TTS ต้องเชื่อมต่อเครือข่าย; ระบบมี fallback เฉพาะ TTS

ส่วน	ไฟล์หลัก
OCR	backend/app/api/ocr.py
Registry	backend/app/services/ingredient_registry.py
PubChem evidence	backend/app/services/pubchem_evidence.py
AI and TTS	backend/app/api/chat.py, backend/app/api/tts.py
Frontend	LabelScanModal.tsx, VoiceAssistant.tsx, SubstanceHoverCard.tsx
Clone check	scripts/verify-clone-ready.ps1

สรุป

ระบบพัฒนาโดยให้ traceability มาก่อนความครอบคลุม: อ่านซ้ำอย่างควบคุม เชื่อมชื่อด้วยหลักฐาน แยก QSAR eligibility ชัดเจน และให้ผู้ใช้ยืนยันทุกการเปลี่ยนสูตรจาก AI