// ART-HLC-024 · PUBLISHED 11 NOVEMBER 2026

How Healthcare Rules Shape MAX4, Then MAX5 Consumer and MARA Healthcare: Law First, Architecture Second

Healthcare rules decide the structure of MAX4, MAX5 and MARA before any code does, and a licensed professional stays in the middle of every decision that matters.

Jason Newell · MAX Research Collective · Article ART-HLC-024 · Published 11 November 2026
Licensed under the Creative Commons Attribution 4.0 International License (CC BY 4.0), https://creativecommons.org/licenses/by/4.0/
Original: https://www.maxresearchcollective.com/articles/how-healthcare-rules-shape-max4-then-max5.html
Cite as: Newell, J. (2026). How Healthcare Rules Shape MAX4, Then MAX5 Consumer and MARA Healthcare: Law First, Architecture Second. MAX Research Collective, ART-HLC-024. https://www.maxresearchcollective.com/articles/how-healthcare-rules-shape-max4-then-max5.html

MAX4 is in progress, MAX5 is the planned consumer release and MARA the planned healthcare version; the healthcare rules they'll answer to are shaping their design before the code does, and nothing here claims a finished product or compliance with any law.

Information, not advice. This article is general information about how healthcare rules can shape software design. It isn't legal advice, it doesn't create an attorney-client relationship, and it isn't a statement that any product, feature or organization complies with any law, standard or program. MAX4, MAX5 and MARA are research and design projects: features described may not exist, may change, or may never ship, and statements about what a design "aims to" do are goals, not assurances. Legal information is current as of 10 November 2026; laws, guidance and litigation change, and readers should consult a lawyer about their own situation. This article hasn't been reviewed by a lawyer. The project is US-only and doesn't address the laws of other countries.

Scope. This article is about how rules shape software design. It does not describe, offer or claim any product or service for use with Medicare, Medicaid, the Children's Health Insurance Program, TRICARE, the Federal Employees Health Benefits Program, Department of Veterans Affairs programs, health insurance Exchange (marketplace) plans, or any other federal or state health care program, or with Medicare Advantage or Medicaid managed care plans. MAX4 and MARA are research and design projects. They do not submit claims to, or seek coverage or reimbursement from, any such program, they do not make or support coverage or payment determinations for one, and nothing here says that any feature is eligible for, supports or complies with the rules of any such program. Billing, claims and payer topics appear only to explain how rules shape design. Nothing in this article is a statement about whether any claim is payable or correctly coded. Any future product for those uses would be described separately, and only after legal review.

Sample data, names, organizations, identifiers and amounts in the figures are fictional; any resemblance to a real person or organization is unintended. Product, standard and company names (including HL7, FHIR, DICOM, SNOMED CT, LOINC, CPT, SOC 2, HITRUST and Llama) belong to their owners and appear for identification only. The Scope above applies to MAX5 in the same terms as to MAX4 and MARA. Written by the MAX Research Collective with AI assistance. Last updated 10 November 2026.

What the rules decide

Healthcare software answers to more rule-makers than almost any other kind of software: federal statutes, federal agencies, fifty states, industry standards, license holders, and the hospital buyers who enforce all of them by contract. An AI model inside the product, reading notes and drafting suggestions, brings rules of its own. Many of those rules constrain the structure of a system rather than its behavior, which is why the Collective reads them before choosing an architecture.

That's the method the Collective is trying with one resident in three stages, an assistant it calls a resident because it lives on one machine:

- MAX4, in progress. A research prototype of a household assistant for a Windows PC, in development since October 2026 and working on synthetic data only.

- MAX5, planned. The consumer release MAX4 leads to, and the first stage designed to handle real consumer health data.
- MARA, planned. The Medical Agentic Resident Assistant, the healthcare version the Collective is designing to sit on the same resident for clinics and hospitals.

The method is to read the rules first, write them down as requirements, and let them shape the design. The hard cases are imaging, helping providers without taking their place, learning across patients, and plugging into other people's records. One design rule runs through all of them: a licensed professional stays in the middle of every decision that matters. All of it is design intent for those three stages, and no part of it is a finished, audited or certified product.

Why healthcare software is different

Most software meets a handful of laws: consumer protection, privacy, perhaps payments. Healthcare software meets those, then a stack that depends on who the customer is, what the data is, what the software claims to do and where the user lives. The same feature can be an ordinary tool in one setting and a regulated medical function in another. Four facts usually decide which:

- Who holds the data, and in what role. A household keeping its own records sits in a different position from a clinic's vendor, and a clinic's vendor from a hospital's. HIPAA, the federal Health Insurance Portability and Accountability Act, speaks of covered entities (health plans, clearinghouses and most providers) and business associates (vendors handling health information for them). Which one an organization is depends on the facts of each arrangement: what it does, for whom, with what data. So the role has to be assessed for each data flow rather than once for the company.
- What the software is said to be for. The Food and Drug Administration (FDA) looks at intended use, and labeling, advertising and design all count toward it.
- What the software does to the decision. Showing a clinician the basis for a suggestion is treated differently from analyzing an image, and differently again from telling a patient what to do.

- Where the person is. State law varies sharply on health data, biometrics, AI disclosure and AI in care.

The rule-makers, in five layers

As of 2 November 2026 the Collective's working requirements register lists 490 numbered requirements, drawn from about 1,500 catalogued sources across federal law, FDA, standards bodies, the fifty states and the District of Columbia. It's a research register. It isn't a legal opinion or a compliance determination, and it may be incomplete or out of date. The requirements fall into five layers.

Federal privacy, security and breach law

- HIPAA's Privacy, Security and Breach Notification Rules (45 CFR Parts 160 and 164, in the Code of Federal Regulations) govern protected health information (PHI) held by covered entities and their business associates: minimum necessary use, the patient's right of access and to an accounting of disclosures, audit controls, unique user identity, breach assessment and notice. The Department of Health and Human Services (HHS) proposed a major Security Rule update on 6 January 2025 (90 FR 898) that would, among other changes, make encryption required rather than "addressable." As of 10 November 2026 it's still a proposal, and HHS's 2026 regulatory agenda puts final action no earlier than July 2027, and agenda dates are estimates. The Collective tracks it as a design reference.
- HITECH, the Health Information Technology for Economic and Clinical Health Act (Title XIII of Public Law 111-5), extended HIPAA's obligations and penalties directly to business associates, added breach notification (now 45 CFR 164.400 to 164.414) and set tiered civil penalties.
- FTC Act section 5 and the FTC Health Breach Notification Rule (16 CFR Part 318) reach past HIPAA. Consumer health apps outside HIPAA still answer to the Federal Trade Commission for deceptive or unfair practices and, if they're vendors of personal health records, for breach notice. Any claim a product makes has to be true and substantiated, and the FTC has brought health-privacy cases against companies whose data practices contradicted their promises.

- 42 CFR Part 2, which covers substance-use-disorder treatment records with stricter consent and redisclosure rules than HIPAA. The final rule of 16 February 2024 aligned parts of it with HIPAA, with a compliance date of 16 February 2026.
- COPPA, the Children's Online Privacy Protection Rule (16 CFR Part 312, amended in 2025), protects children under 13, and E-SIGN governs electronic consents and notices that the law requires in writing.
- Section 1557 of the Affordable Care Act (45 CFR 92.210) reaches decision tools. Covered health programs and activities must make reasonable efforts to identify the patient care decision support tools they use whose input variables measure race, color, national origin, sex, age or disability, and reasonable efforts to mitigate the risk of discrimination from them. AI tools are within its scope.

Federal rules for the product itself

- FDA and the decision-support exclusion. Section 520(o)(1)(E) of the Federal Food, Drug, and Cosmetic Act (21 USC 360j(o)(1)(E)), added by the 21st Century Cures Act, takes some clinical decision support (CDS) software outside the medical-device definition, and only when it meets all four statutory criteria. As the Collective reads FDA's final CDS guidance (issued 6 January 2026 and re-issued 29 January 2026), software that analyzes a medical image or a signal falls outside the exclusion, so does software advising patients or caregivers rather than clinicians, and software for time-critical decisions doesn't meet the fourth criterion. FDA's General Wellness policy (revised 6 January 2026) covers low-risk products for healthy-lifestyle purposes, and it stops where a product claims to screen, diagnose, monitor or manage a disease or presents its outputs in a diagnostic context. Readers should check the guidance itself.
- Device-maker duties, if a function does become a device. They include a quality system under the Quality Management System Regulation (QMSR, aligned with ISO 13485), risk management (ISO 14971), a software lifecycle (IEC 62304), usability work, a cybersecurity file with a software bill of materials (SBOM), a premarket route such as a 510(k) or De Novo request, a predetermined change control plan (PCCP) for model updates, registration, listing and adverse-event reporting.

- ONC and the Cures Act information-blocking rules (45 CFR Part 170 and Part 171, with Part 172 for TEFCA, the Trusted Exchange Framework and Common Agreement). The Office of the National Coordinator for Health IT (ONC) bars "actors" from unreasonably interfering with access to electronic health information, subject to defined exceptions. ONC's HTI-5 final rule (Federal Register document 2026-21943, 91 FR 67916, published 28 October 2026 and effective 28 December 2026) removes the earlier certification requirement for decision-support "source attributes." The Collective keeps that model-card metadata anyway.
- CMS interoperability and prior authorization rules (CMS-0057-F and the HTI-4 criteria) for payers' electronic prior-authorization interfaces and decision clocks, and the No Surprises Act for good-faith estimates and balance billing. These are obligations of payers, plans and providers. The Centers for Medicare & Medicaid Services (CMS) rules appear here only to explain design (see Scope).
- Federal standards for transactions and codes: HIPAA's adopted X12 transactions, ICD-10, HCPCS and NDC, with CPT owned and licensed by the American Medical Association (AMA).

State law

State law moves fastest, and it differs from state to state.

- Consumer health data. Washington's My Health My Data Act (RCW 19.373) requires consent to collect, separate consent to share and a valid authorization to sell, and it carries a private right of action. Nevada SB 370 and Connecticut's consumer health data provisions follow similar lines. California's Confidentiality of Medical Information Act (CMIA) can make a business that offers consumers software to manage medical information a "provider" under it, and the California consumer privacy law's rules on automated decision-making phase in from 2026 to 2027. These laws reach health data HIPAA doesn't cover, which is where consumer apps usually sit. Oregon's consumer privacy act (ORS 646A.570 to 646A.589) treats mental or physical health conditions and biometric data as sensitive data that needs consent once its volume thresholds are met, and it exempts only protected health information handled under HIPAA, leaving a person's other data in scope.

- Biometrics. Illinois's Biometric Information Privacy Act (BIPA) requires a written release and a retention policy and carries a private right of action; it exempts information captured from a patient in a health care setting or collected for HIPAA treatment, payment or operations. Colorado has its own biometric duties, and Texas and Washington have statutes their attorneys general enforce. A voiceprint is a biometric identifier, which matters for a resident that learns who is speaking. Portland, Oregon also bans private use of face recognition in places of public accommodation in the city (Portland City Code 34.10), with a private right of action, which matters for any clinic waiting room.
- AI in care and AI disclosure. As of 10 November 2026: Texas's TRAIGA (HB 149) has providers disclose AI use, and Texas SB 1188 has practitioners review AI-generated records and keep electronic health records stored in the US. Utah has AI disclosure rules (Utah Code 13-77-103) and mental-health-chatbot rules (Chapter 72a). Illinois HB 1806 bars AI-delivered therapy. Oregon SB 1546 covers companion chatbots from 1 January 2027, and Oregon HB 2748 limits non-human use of the title "nurse." Colorado SB 26-189, signed on 14 May 2026, replaces the Colorado AI Act from 1 January 2027. A court order of 27 April 2026, entered on the parties' stipulation, bars the Colorado attorney general from starting any enforcement of the earlier act, or of legislation replacing or amending it enacted in that session, for violations on or before 14 days after the court rules on a preliminary-injunction motion that xAI has said it will file in X.AI LLC v. Weiser. The Collective keeps these as a maintained list with review dates, since federal preemption moves are also in play.
- State prior-authorization and AI-in-review laws, along with state insurance regulators' data-security and AI bulletins, apply to anything that touches payers.

Standards, frameworks and certifications

These are mostly voluntary in law and required in practice, because hospital buyers ask for them: SOC 2 Type II, HITRUST, ISO/IEC 27001, ISO/IEC 42001 (an AI management system), the National Institute of Standards and Technology's AI Risk Management Framework (NIST AI RMF) and its generative-AI profile, NIST's Secure Software Development Framework, NIST biometric accuracy guidance, WCAG 2.2 accessibility, FIPS 140-3 for cryptographic modules, and, for government buyers, FedRAMP and

CMMC. Interoperability standards bring their own conformance work: HL7 FHIR with US Core, HL7 v2, C-CDA, DICOM and USCDI, each glossed where the article reaches integration.

Licenses and contracts

Contracts and licenses bind software as firmly as statutes do. CPT descriptors need an AMA license. LOINC and SNOMED CT have their own terms. Open-weight models carry licenses with acceptable-use policies and notice duties, the Llama community license among them. Vendor API terms, app-store rules, email-provider verification programs and the business associate agreements (BAAs) a hospital signs all constrain what software may do, and with what data.

What changes when the product has AI inside

An AI model that's part of the product, rather than a tool sitting next to it, raises questions the older rules didn't anticipate.

- Intended use stops being fixed by a feature list. A model can be asked anything, so what the product says it's for and what its design lets it do both count. A resident that can be asked for a diagnosis needs a design that's built to decline to give one.
- The FDA line is about function. The decision-support criteria turn on what the software reads (text and reported results, or images and signals), who it speaks to (a clinician, or a patient), and whether the reviewer can see the basis and weigh it independently. The Collective's designs call for labeled insights carrying their basis, evidence grade and confidence, with a person accepting, editing or rejecting each one.
- State AI laws read like disclosure and review rules. They ask a product to say it's an AI, to let a licensed person review what the AI drafted, to keep records for years, and to offer correction and human review for consequential decisions.
- Bias review is part of the design. Section 1557 and state anti-discrimination law reach the covered program's use of the tool, so the Collective treats identifying

and mitigating bias, including evaluation by subgroup, as a design practice from the start.

- Learning on real data can move a function across a regulatory line. That's why the design treats model updates as change-controlled events with a log.
- Security changes shape. An agent that can act raises "least agency" questions, prompt-injection defense, supply-chain questions for every model and package, and adversarial testing before each release.
- The model has a provenance. Who made it, under what license, on what data, and whether it can be removed if its training turns out to have been improper.

A professional in the middle

One rule runs through every layer above, and the Collective treats it as a design rule: in the design, a licensed professional is in the middle of every decision that matters.

The law points the same way from several directions. FDA's decision-support exclusion depends on a clinician being able to review the basis for a suggestion independently rather than mainly relying on it (section 520(o)(1)(E)(iii) and (iv)). Texas SB 1188 expects a practitioner who uses AI for diagnosis to review every AI-created record and to disclose the use. California's rule for generative-AI patient messages relaxes its disclaimer only when a licensed provider has read and reviewed the message (AB 3030, Health and Safety Code 1339.75). Several states' insurance laws on AI in coverage decisions keep an algorithm from being the one that denies or downgrades care. Colorado SB 26-189, from 1 January 2027 and subject to the court order above, asks for notice at the point of interaction and a right to correct the data an automated tool used, and requires developers to give deployers documentation that includes instructions for human review. Section 1557 makes the covered program answerable for the decision support tools it uses. And a signed report belongs to the physician who signed it.

So the design puts a professional in the middle in four concrete ways:

- Each insight is designed as a proposal. In the design, it carries its basis, evidence grade, confidence and cohort size, and a professional accepts, edits or rejects it. The same trust ladder, the graded levels of independence a resident's abilities

earn, is designed to govern MAX4, MAX5 and MARA, with no autonomous rung for claims.

- The design leaves signing to a person. An entry counts when a responsible person signs it, and MARA is designed with no signing role.
- Friction is deliberate. A ”sign as-is” button invites automation bias, the well-studied habit of trusting a machine’s output too readily. The design favors a persistent draft banner, review of each section and, when a reader rejects a high-confidence AI finding, a short recorded reason.
- Actions are designed to be logged. In the design they’re also reversible where the system controls the other side, and a person can lower an approval gate while the audit trail stays on.

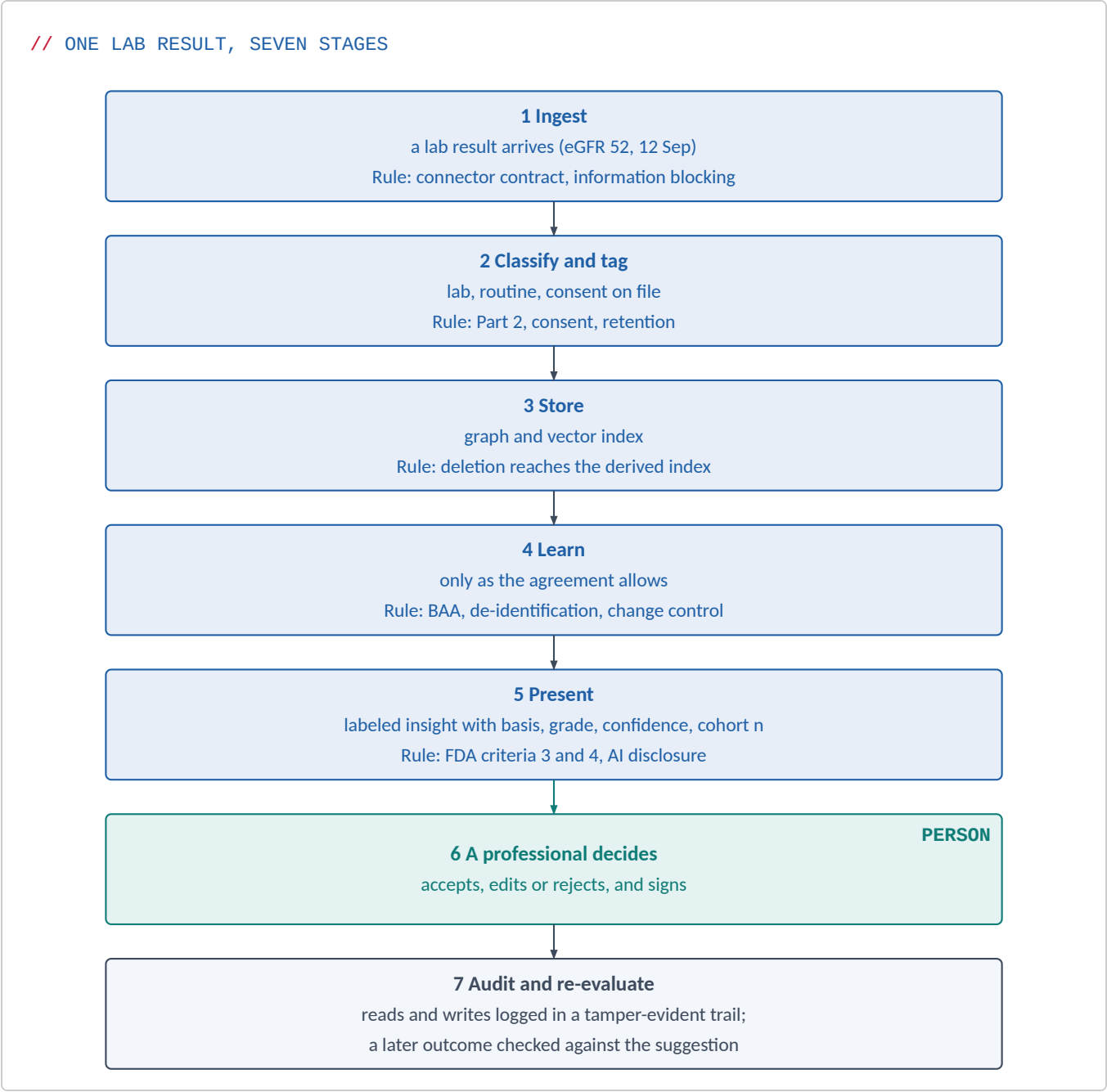


Figure 1. One lab result through seven stages: software and AI work at stages 1 to 5 and 7, and a professional decides at stage 6. Invented data.

A professional in the middle is also the cheapest way to stay on the right side of the FDA line, though it doesn't replace that line. A professional signing an image-derived draft leaves the draft in device territory; what the signature changes is who answers for the result.

The ambition: one learning system from triage to follow-up

The point of building MARA is better information at each step of care, drawn from what AI does well: learning from many patients at once. The design uses vector embeddings of notes, results and events (numeric fingerprints that let similar records be found together), a knowledge graph tying patients, visits, orders, findings, providers and outcomes to each other, and cohort statistics drawn across both. The aim is one resident who follows the care journey from a patient's first contact through triage, scheduling, the exam, diagnostics and follow-up. The MAX4 prototype is where the working method is being developed, a local knowledge graph and similarity index kept in step with one canonical copy of the data, and MARA would apply it to clinics, hospitals and specialists. It's the Collective's research direction, and it describes no shipped product.

The law allows this ambition in parts: some a professional may be shown, some need a regulator's review first, and some stay off limits. The Collective's research sorts each step of the care arc into assist-only (a professional decides), its own FDA path, open, and off limits as designed, and it marks two steps as outside this article, billing as not offered and payer-side review as research only. At home the value is the person's own contribution to their record, with diagnosis kept off limits. Table 1 gives the research view, with invented examples.

Table 1. The care arc, step by step, as the Collective's research frames it. Invented examples.

STEP	EXAMPLE VALUE-ADD	WHERE IT LANDS
Scheduling, front desk, price estimates	Suggests a slot or a price estimate; accuracy duties under price-transparency and No Surprises Act rules stay with the customer	Assist-only
Guideline checks from text and reported results	Shows which guideline criteria a lab panel meets, with the sources	Assist-only, with the basis shown
Medication checks	Interaction and formulary displays	Assist-only; a pharmacist or prescriber decides
Treatment options	Lists guideline options with citations; the clinician chooses and the choice is logged	Assist-only, with a Section 1557 bias review
Risk scores and early-warning alerts	A deterioration score from chart data	Open, and defaulting to an FDA path, because a time-critical alert the clinician can't independently weigh has been treated as a device
Anything that reads pixels, waveforms or other signals	Triage, markup or drafting from an image or an ECG	Needs its own FDA path
Patient at home, with MAX5	Records what a person says about their health, in their words and dated, and with their permission sends it as patient-reported information to the clinic's EHR where that system accepts it, or to MARA; either way it can print a visit summary to bring along	Assist-only for the person's own record; a diagnosis ("your symptoms suggest X") is off limits

STEP	EXAMPLE VALUE-ADD	WHERE IT LANDS
Billing and payment	Outside the scope of this article (see Scope)	Not offered
Payer-side review	Neutral evidence display and completeness checks for a human reviewer	Research only; not offered for any government program



Figure 2. Table 1's steps as eight cards, with medication and treatment combined, and the Collective's research view of what the rules let AI do at each step. Invented examples.

Imaging: where the complexity concentrates

Imaging is the hardest part of the care arc, for three reasons that stack.

First, the law treats pixels differently from words. The first of the four decision-support criteria excludes software that acquires, processes or analyzes a medical image or a signal. Once software reads an image it's outside the exclusion, whoever signs afterwards. The Collective's research maps the territory onto FDA's existing product codes, the three-letter labels FDA uses to classify device types: worklist triage and notification (QAS, QFM), detection and markup (MYN, QIH), and characterization of lesions (POK). Devices of these types typically reach the market by a 510(k); QIH, for example, is a Class II code under 21 CFR 892.2050 and covers non-adaptive algorithms only. In the Collective's research, drafting a report from an image has no dedicated product code. Whether FDA has authorized any device that drafts a report from an image is a question for FDA's public databases, and this article doesn't answer it. Designations such as Breakthrough aren't clearances.

Second, both ways to market have traps. A company can seek its own authorization, which brings a quality system, risk management, usability work, a cybersecurity file, reader studies that measure the radiologist and the AI together, registration, listing and adverse-event reporting. Or it can license a cleared component and stay inside its labeled use; if the company's layer adds clinical content the cleared device didn't produce, though, the combination is likely a new or modified device. A learning model adds change control. FDA's PCCP lets a maker agree in advance how a model will be updated, and at least one product code is limited to non-adaptive algorithms.

Third, responsibility has to be split honestly. The radiologist who signs answers for the report. The facility answers for choosing, training and monitoring the tool. The vendor answers as a maker for design defects and failure to warn. Contracts can shift part of that responsibility between the parties, though no contract disclaims all of it.

So the Collective's design decisions are these. MARA's core is designed to work from text and reported results only. Image and signal analysis would be a separate, later, deliberate function needing its own FDA path (a premarket route, a change-control plan and registration). It isn't part of the core, and nothing in this article says any

such function exists or is cleared or approved. Helpers for radiology that read no image stay in the core as assist-only: structured templates, prior-report retrieval, lookup of appropriateness criteria from the order text, and tracking of follow-up recommendations.

How help is shown to providers

How the help is worded and shown is partly a legal matter, because FDA, the states and plaintiffs' lawyers all read the screen.

- Say what it is. In the design, each insight is labeled as AI-generated and not established fact, with its basis, evidence grade, confidence and the cohort size behind it. The design shows no per-patient risk score without that basis.
- Offer options. In the design, the product's words are options, evidence and "for your consideration," "recommends" is kept out, and the professional's choice is recorded as theirs, under their name.
- Show the basis in one step. A "Review basis" view is designed to let the clinician check the sources and the inputs independently, which is what the fourth criterion asks for.
- Make review real. A persistent draft banner, section-by-section review and no one-click sign-off. For a rejected high-confidence finding, the design sends a short structured reason (not present, benign, artifact, other) to the quality record rather than the patient's report.
- Disclose where the law asks. As of 10 November 2026, Texas expects providers to tell a patient when AI is used in a service; California asks for a disclaimer on generative-AI patient messages that no licensed provider reviewed; Utah and others add their own banners. The Collective plans a disclosure template for each state.
- Keep payer-side screens neutral. The research design shows evidence and completeness checks to the human reviewer and sorts nothing by likely outcome.
- Tell clinicians what's measured. Where their edits feed learning, the design calls for a first-use notice saying so and saying who can see it.

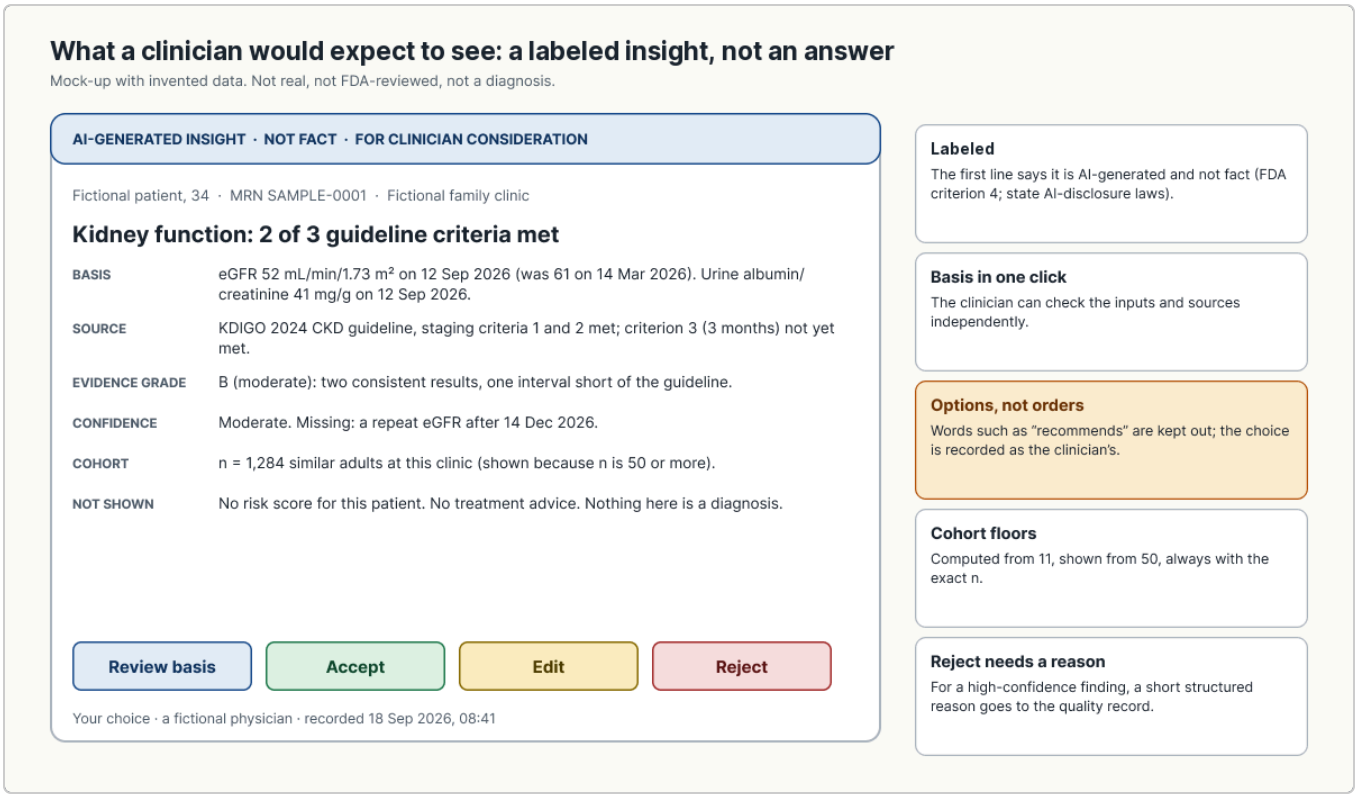


Figure 3. What a clinician would see in the design: a labeled insight with its basis, and choices that are the clinician's. Mock-up with invented data.

At home: a guide that helps you tell your doctor

Everything above is about the clinic. The consumer resident, MAX4 now in progress and MAX5 as the planned consumer release, has a different job and different rules. His most useful habit is one a good attending caregiver has: he pays attention to what a person says over days, writes it down, and helps them bring the right things to the right person at the visit.

In the design, the home resident does four things with what a person says or describes about their health, and the fourth is the point of the other three: it helps the person contribute to their own health record.

- Remembers it, in their words and with the date. "Fri 18 Sep: I fell off the curb and couldn't take four steps."
- Organizes it for the visit. A short list for the appointment on the calendar holds what was said, when, and what the person asked, with a plain prompt for the details a clinician usually wants (which toes, how often, what dose).

- Prompts rather than interprets. It says ”tell your doctor,” and the design keeps it from saying what the symptom means, what caused it or what to do about it.
- Gets it into the record, the way the person chooses. MAX5 is planned to offer three routes, each one used only when the person says so. Where the clinic’s EHR accepts patient-entered information from an app the person authorizes, MAX5 could send the stated symptoms there, labeled as patient-reported. Where the clinic runs MARA, MAX5 could pass the same list to her for the clinician’s review. And with no connection at all, MAX5 could print a visit summary on paper for the person to carry to the appointment or the hospital.

Figure 4 shows the visit list in a mock-up with invented data; the sending and printing routes aren’t drawn in it. The law is the reason for each of the limits around them.

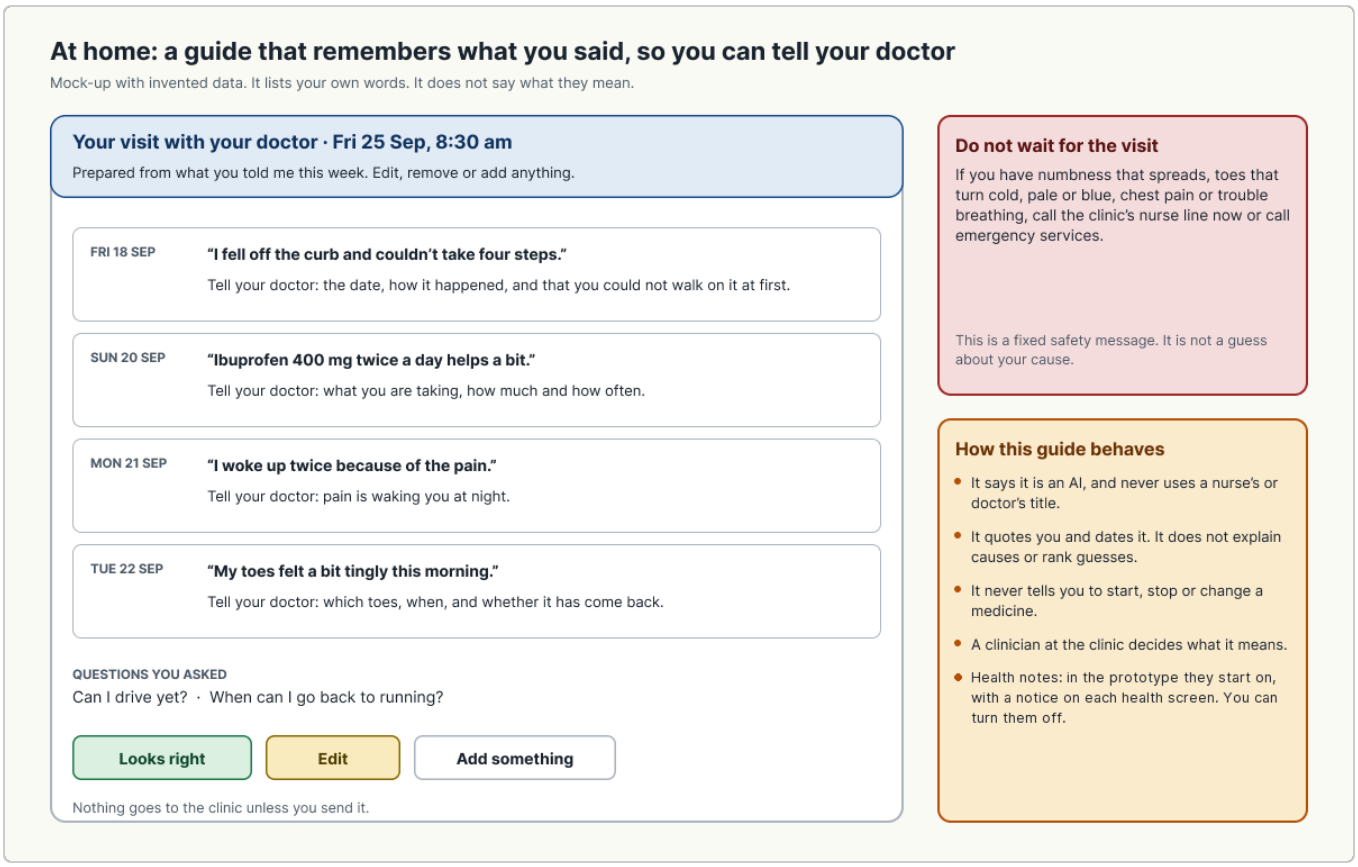


Figure 4. A home guide that lists what a person said and what to tell the doctor. The red box is a fixed safety message rather than a guess about a cause. Mock-up with invented data; the send and print routes aren't shown.

- FDA draws its line at who the software speaks to and what it says. Decision support for patients and caregivers is outside the clinician-facing exclusion, so a feature that said "your symptoms suggest a sprain" would invite a device question and, in some states, a practice-of-medicine one. A feature that records what a person said, dates it and prompts them to share it is, in the Collective's working view, a records-and-navigation function. Whether any function is a medical device is a question for FDA and counsel, and this article doesn't decide it. The design rule is no diagnosis and no prescription at home, and design copy is checked for diagnosis wording.
- A license or title isn't borrowed. The resident is designed to say it's an AI, which several companion-chatbot and AI-disclosure laws require, and to use no "nurse," "doctor" or similar title; Oregon's HB 2748 (2025) separately limits non-human use of the title "nurse." The guide is meant to be a caregiver in manner, with no claim to a credential.
- Red flags are named plainly. In the design, a fixed safety message sends the person to the clinic's nurse line or emergency services for the situations a clinician wouldn't want to wait on, and it's written in advance as a rule rather than left to a model's judgment. The design also plans a crisis referral for mental-health topics.
- Medicine stays the clinician's. In the design, the guide can record "ibuprofen 400 mg twice a day" because the person said so, and prompt them to tell the doctor; the design keeps it from advising starting, stopping or changing a medicine.
- Health notes belong to the person. In the current MAX4 research prototype, health features are on by default for the person using it, with a visible notice on every health screen that it's a prototype, and each person can switch them off. The Collective's plan for MAX5 and any other distributed build is to ask each person to opt in first. Reminders and calendar entries are designed to carry a bare time without health detail, and the design sends nothing to a clinic unless the person sends it. Whether a household install is a covered entity or business associate depends on its facts. In the design the Collective receives none of the household's data and no clinic is involved, consumer-protection and state health-data laws still apply, and the same record is kept ready for when a clinic is involved.

- Writing into a chart is the clinic's call. As of 10 November 2026, the information-blocking rules give patients a right of access to their records, and they don't oblige an EHR to accept what a patient's app writes. So the EHR route exists only where the clinic's system offers a patient-entry path, the vendor's app terms allow it and the clinic agrees, and what arrives is labeled as the patient's own report for a clinician to weigh. An app that keeps a person's health record outside HIPAA can also be a vendor of personal health records under the FTC's Health Breach Notification Rule, with breach-notice duties of its own. The paper summary needs none of that plumbing, which is why the design keeps it as the route that needs no connection at all.
- A professional decides, again. The clinician decides what the list means, and what to share stays the home user's choice.

A guide like this is also where the clinic's side meets the home. The list a person brings is the "reported result" a clinician-facing insight can start from, and in the design it reaches the clinic's record through the person, when they choose to share it: sent from MAX5 into the EHR, passed to MARA, or carried in on paper.

Learning from many patients, and from the past

The value of owning the learning is a system that improves with each visit, each edit and each outcome, and that can look back over its own history for patterns no single clinician sees. The law decides under what authority each kind of learning may happen, as Table 2 sets out.

Table 2. Kinds of learning and the authority each needs under HIPAA, as the Collective's research reads it.

KIND OF LEARNING	WHAT THE LAW ALLOWS	CONDITION
Quality improvement for one customer (error analysis, tuning, dashboards)	Health care operations of that customer, which a vendor acting as its business associate may perform for it	The BAA must list it; minimum necessary applies; the result stays with that customer
Benchmarks across several customers	Data aggregation for those customers' operations	Every participating agreement must permit it; one customer's data isn't disclosed to another
A general model sold to all customers	Closer to research than to a customer's operations	Authorization, an institutional review board (IRB) or privacy-board waiver, a limited data set, or de-identified data; the regulator hasn't squarely addressed whether a vendor's model training counts as operations
Anything shared across customers	De-identification by Expert Determination (Safe Harbor rarely fits images or free text)	The agreement must expressly permit it and say who owns the result; images need DICOM header and burned-in text scrubbing, and free text needs scrubbing plus expert review
The vendor's own business	Narrow	Not a basis for model training

The Collective's working position follows from that table, and it's an open legal question the Collective hasn't yet put to a lawyer. A customer's data would train that customer's instance unless the customer opts in to a de-identified network, in separate clauses. Model weights trained on health data can memorize it, so an exported weight is treated as possibly carrying health information until shown otherwise. Models would be retrained periodically and locked between releases, with per-site tuning only inside bounds agreed in advance and an automatic rollback, and with no continuous online learning inside the clinical path.

Cohorts follow the same discipline in the design: aggregate-only, nothing computed below eleven patients, nothing shown to a person below fifty, exact counts, and a check that two slices can't be subtracted to expose a small group.

Retrospective learning comes in three kinds. Looking back over a customer's own data to improve its care is operations; looking back to produce knowledge for others is research and needs the research route. Looking back over the system's own conduct is a record. In the design, the audit log answers who read a record, when, why, whether reading was held and released, and whether the chain of entries was intact when it left.

Clinicians' own performance raises the same questions. Comparing individual radiologists is a legitimate operation for the facility's peer-review committee, and a vendor has no business doing it across customers. The design keeps an individual view in a restricted peer-review workspace, because ordinary management dashboards may lose peer-review protection, and the planned contract says metrics alone never decide credentialing or employment, since employment-discrimination law and state laws on AI in employment apply.

Getting it integrated: HL7, FHIR, DICOM and the rest

A clinic's patient sits in someone else's electronic health record (EHR), their images in someone else's archive, their insurance records with a clearinghouse. The design speaks the standards that already carry that traffic. Health Level Seven (HL7) publishes FHIR, Fast Healthcare Interoperability Resources, the current web standard for health data, and HL7 v2, the older message format hospitals still run on. DICOM, Digital Imaging and Communications in Medicine, is the standard for images.

Table 3. The standards a connector would have to speak, by kind of traffic. Claims, remittance and prior authorization appear for context only (see Scope).

TRAFFIC	STANDARD
Patient data, apps and APIs	HL7 FHIR R4 and US Core, with SMART on FHIR for app launch
Feeds from hospital systems	HL7 v2 messages (admissions, orders, results)
Documents	C-CDA (Consolidated Clinical Document Architecture)
Images	DICOM, including DICOMweb; PS3.15 de-identification profiles
Data baseline	USCDI (United States Core Data for Interoperability)
Eligibility checks	HIPAA X12 270/271 transactions and CAQH CORE rules
Claims, remittance and prior authorization (context only, outside this article's scope)	HIPAA X12 837, 835 and 278, and payer APIs under CMS-0057-F
Networks	TEFCA through a qualified health information network, optionally

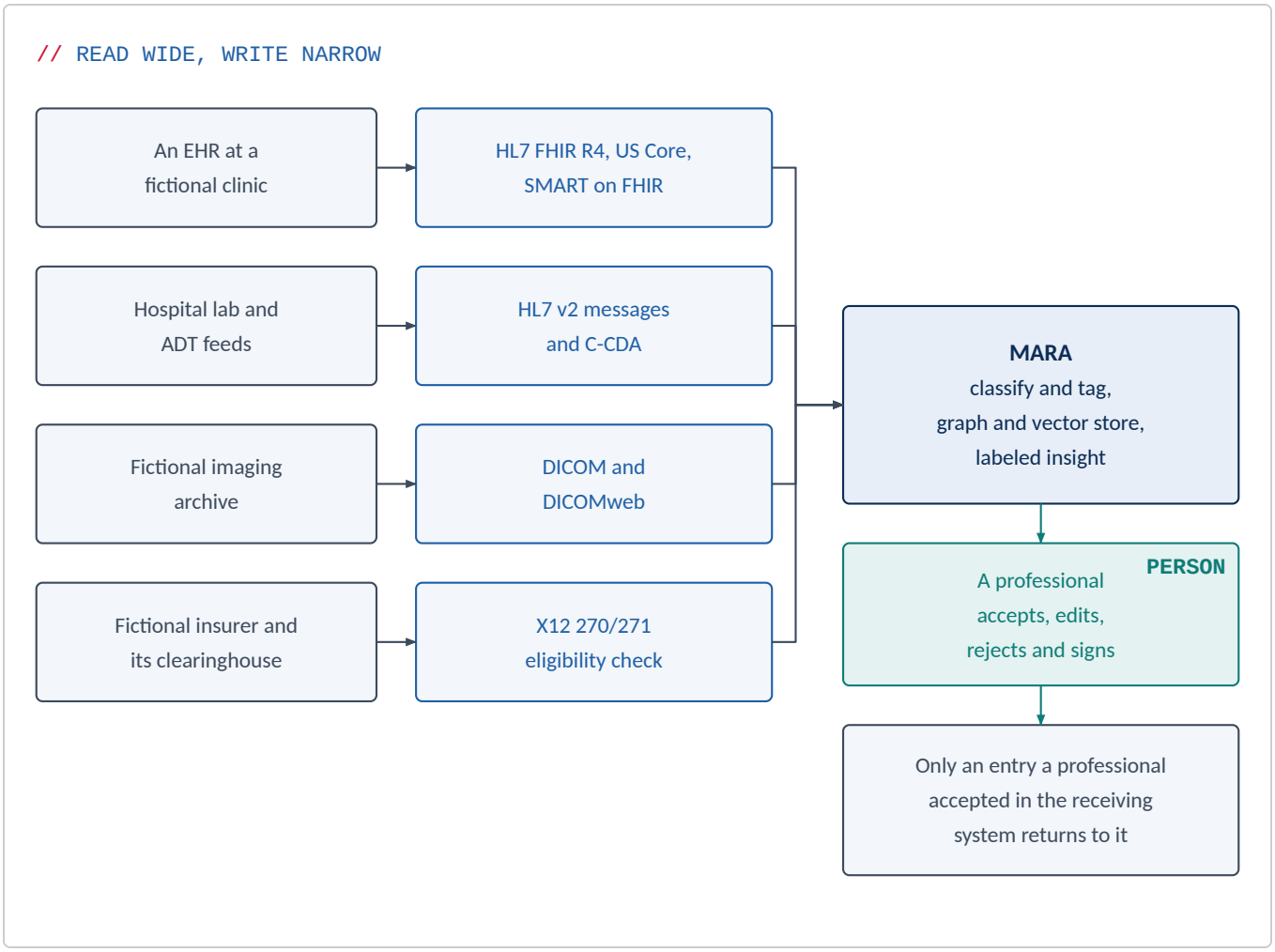


Figure 5. Reading wide through standards and writing narrow: in the design, nothing written back counts until a professional accepts and signs it in the receiving system. Invented organizations.

Integration is also where several laws bite, and the design treats each as a constraint on how the plumbing is laid:

- Information blocking. Health care providers that are customers are ”actors” under the Cures Act rules, and a vendor can be one too, depending on what it offers. A portal gate that holds actions for review must leave a patient’s electronic access to their own record undelayed unless a defined information-blocking exception applies and is documented.
- Sensitive records arrive without labels. ONC’s HTI-5 removes the certification criteria for security labels, so an EHR is no longer required to be certified to send a substance-use or reproductive-health tag, and the design can’t count on receiving one. The design derives the tag from source metadata at ingest.

- Vendor terms: EHR and imaging vendors write their own API terms, and app-store and email-provider rules add more, so each connector is a contract as well as an interface.
- Terminology licenses: CPT, LOINC and SNOMED CT carry terms a connector has to honor.
- Patient matching: a wrong link between two people's records puts one person's results in the other's chart, so matching is treated as a safety question.
- Plan-installed first. By design the software runs in the customer's environment, with per-site learning kept on site. Whether the vendor is a business associate depends on what access it has (remote support, logs, updates and model calls can all create access) as well as on where the data is stored, so customers should sign a BAA if the vendor has any access to protected health information.
- Read wide, write narrow. In the design, the resident reads through standard interfaces and writes back only labeled drafts, which count once a responsible person accepts them in the receiving system, and she has no role in authenticating a chart entry.

How the Collective gets it done

The pipeline the design follows is the same at every step, and each stage is where a rule attaches:

- Ingest through standard interfaces, under the connector's contract.
- Classify and tag each field and record on arrival: sensitivity, source, consent, retention.
- Store in the graph and the vector index, with the graph's canonical copy deletable so that deletion reaches the derived index.
- Learn only through the path the agreement and the law allow, and only in locked, change-controlled releases.
- Present as a labeled insight with its basis.
- Decide: a professional decides, and the decision and its reason are recorded.

- Audit and re-evaluate: reads and writes are logged in a tamper-evident chain, and an outcome that misses demotes the ability that produced it.

The order of work follows the gates. Synthetic patients come first, in MAX4, then real consumer data with MAX5, then real patient data in MARA only after leadership sign-off and review by a qualified lawyer, then the clinic, hospital and later stages, with the FDA track kept separate for anything that reads an image or a signal. Each stage meets the rules that begin there. Billing and government-program stages are outside the scope of this article (see Scope). Today the MARA demonstration runs on invented patients only, and it connects to no real record, payer or EHR.

Why the rules come before the architecture

The usual order in software is to pick a stack, build features, then ask what the lawyers will say. In healthcare that order is expensive, because many rules constrain structure. A rule that says "log reads as well as writes" can't be satisfied by wrapping a finished system in a logger; the data layer has to know who is reading what, and for what purpose. A rule that says "tag substance-use-disorder records at ingest" can't be met if the data model has nowhere to hang a sensitivity class. A rule that says "show the clinician the basis for each suggestion" is a screen design, a data model and a retrieval design at once.

So the Collective worked in the other order. It built the requirements register first: the laws, standards and licenses it could identify, each mapped to the product versions it applies to and to the gate where it starts to bite. The register is a research tool, and it's neither complete nor audited. Then the architecture was checked against the register, and the register was allowed to change the design. Table 4 shows the pattern.

Table 4. Rules and findings, and what each did to the design.

RULE OR FINDING	WHAT IT DID TO THE DESIGN
FDA decision-support criterion 1: text and reported results only, no image or signal analysis	MARA's design reads written reports and reported values. Image and signal analysis is set apart as a later, separate function on its own premarket path.
FDA criteria 3 and 4: options for a clinician, basis shown, no automation bias	Each insight card in the design carries its basis, evidence grade and confidence, and a professional accepts, edits or rejects it. The word "recommends" is out of the product's copy.
No diagnosis or prescription at home	A consumer-facing resident is designed to reframe such requests as questions to bring to a clinician.
HIPAA audit controls (45 CFR 164.312(b)) and the right to an accounting	The audit design treats a read as an event: tamper-evident, with a "who looked" view as well as a record of changes.
Information-blocking rules	A portal gate must leave a patient's access to their own record unblocked unless a documented exception applies.
Part 2 and reproductive-health sensitivity	In the design, records carry a sensitivity class from the moment they arrive, derived from source metadata because EHRs may not send labels.
Small-cell re-identification risk in cohort statistics	The cohort design is aggregate-only, computes nothing below a floor of 11, shows nothing below a floor of 50, states the exact n, and checks for differencing between slices.
BIPA and state biometric law	Design aim for MAX5 and MARA: ask each person before keeping a voice or face template, with a retention rule and deletion on request, and a voice alone doesn't unlock anything without the PIN. The MAX4 research prototype isn't offered for general use and handles voice samples differently.
HTI-5 drops the model-card requirement while state AI-	The design keeps model-card metadata regardless.

RULE OR FINDING	WHAT IT DID TO THE DESIGN
in-decisions laws ask for the same documents	
Payer-side research: the Collective's working position is software-only	The design avoids any function that would need a third-party-administrator or utilization-review license, an assumption to confirm state by state. In the design a professional presses send, and the trust ladder has no autonomous rung.
HIPAA roles are decided per data flow	The design gives each store a declared posture, and the first real-data gate waits for leadership sign-off and review by a qualified lawyer.
Hospital buyers ask for SOC 2, SBOMs, penetration tests and AI governance packs	The build is designed to be able to produce them: pinned, hash-checked components, an SBOM for each build, dependency scanning and a written model register.

Three habits hold the method together.

- Constraints are decisions, written down. Each leadership ruling that limits the design (synthetic data only for now, text-only inputs, a professional always decides) goes into a decision log the registers point to, and a later change has to go through the same log.
- The architecture is allowed to lose arguments. When the register and a design disagree, the register is checked first. Where the design wins, the reason is recorded; where the rule wins, the design changes.
- Scope is a legal tool. Local-first design, synthetic data and a household-only deployment narrow which rules apply at each stage. It's a way of meeting each rule at the stage where it starts to apply, in the order the Collective calls gates.

The gates

The Collective sequences the work in gates, so no rule is left to the last minute and none is built long before it applies:

- Now, MAX4 in progress: the research prototype and the MARA demonstration, synthetic patients only.
- MAX5, the consumer release, with real consumer health data: state consumer-health and biometric consent, the FTC breach rule, each EHR vendor's terms for patient-authorized apps, encryption of every store, telemetry off by default, children's rules.
- MARA, first real patient data: leadership sign-off, review by a qualified lawyer, a decided contracting entity, de-identification for anything leaving the clinic.
- First clinic: BAAs, a HIPAA risk analysis, a breach process, AI disclosures, Section 1557 inputs, cyber insurance, SOC 2 readiness.
- First hospital system: SOC 2 Type II, a penetration test, FHIR and EHR vendor programs, information-blocking design, an AI governance pack.
- Billing and payments (outside the scope of this article): not offered; any future function would be reviewed separately before it's designed.
- First payer pilot (design research only): the software-only position, prior-authorization interfaces and clocks, state AI-in-review laws.
- Government buyers (future): FedRAMP or GovRAMP and Section 508; any representations made to federal buyers would need separate legal review.
- FDA track, separate: any image, signal or time-critical function.

Design intent for MAX4, MAX5 and MARA

The Collective keeps an internal checklist of design intent against its register, and it asks one question of each rule: is it held for a later stage, planned in a limited form that moves toward the rule, or planned in full? This section summarizes that thinking at a high level. It's a design self-assessment dated 2 November 2026, it has changed since, and it isn't an audit, a certification or a statement that any product complies with any law. For MAX4, a household research prototype in progress, and for MAX5, the planned consumer release, HIPAA's rules serve as design references; whether HIPAA applies to any deployment depends on its facts.

Held until MARA

MAX4 is the resident in progress and MAX5 the consumer release it leads to. Some rules belong only to a hospital, a clinic, a payer or a device maker, and the design places them in MARA by decision, so the consumer line stays small and each rule is met where it applies.

- Hospital interfaces. HL7 v2 feeds, C-CDA documents, a USCDI-mapped data model and DICOM imaging exchange belong to MARA's stage. In the MAX4 prototype, FHIR appears only as copy in the synthetic clinic preview.
- Billing and payer functions are outside the scope of this article (see Scope), and none of it is in MAX4.
- Buyer-facing governance. Hospital AI governance packs, vendor security questionnaires, ISO/IEC 42001 certification and an ISO/IEC 27001 management system are MARA's to show buyers, and the MAX4 prototype is planned to supply raw material for them.
- Device-maker machinery. Design reviews with independent reviewers, a device master file, a safety classification for each software item, a surveillance plan and FDA's draft lifecycle recommendations for AI-enabled devices wait for the first function that could be a device.
- Organization-level duties tied to real data. Naming a HIPAA security official, workforce training records and patient matching wait for the first real health records, and FIPS 140-3 validated cryptography waits for a buyer who asks.

Planned in a limited form first

For these the Collective chose a smaller, safer form that moves toward the rule. They're design goals in progress, and none of them is a completed control.

- Software distribution and updates. Integrity checks on installers and updates are being built in stages; publicly trusted signing and authenticated updates are planned for the first public distribution.
- Encryption. Sensitive local stores are designed to be encrypted, and the aim is for every store to be encrypted before any real health data is handled.

- Synthetic clinic data. The prototype's clinic preview uses invented patients, a fixed SYNTHETIC banner and made-up identifiers, designed so its screens don't pass for real ones.
- Decision-support criteria. The preview is designed to show the basis, grade and confidence of each insight and an accept, edit or reject choice; the retrieval and citation machinery behind it belongs to MARA.
- No diagnosis, no prescription. Design copy is checked for diagnosis wording, and further safeguards on the model's own output are planned.
- Local services. The local model and vector services are designed to run on the device only.
- Cohorts, consents and sensitivity tags. In the prototype, the cohort floors are written into a specification and tested, and the engine that enforces them is planned for when there are real cohorts. Consent and sensitivity tags for Part 2 and reproductive health appear as copy until there are stores to hold them.
- Licenses. In the prototype, model and voice licenses are tracked and carried with notices, and the design keeps non-commercial components out; further checks on terminology and model licenses are planned.
- Quality system. For now the prototype runs a lightweight lifecycle (a regression test for each bug fixed, checked releases, a decision log); the formal IEC 62304 and QMSR processes would be written when a function becomes a device function.
- Telemetry and analytics. Any collection is planned to be described in a privacy notice before it applies to anyone outside the project.
- NIST AI RMF. The Collective has mapped the framework and its generative-AI profile as a design reference.

Planned in full for MAX5, the consumer release

The design for MAX5 aims to include the following controls, carried forward from the work in MAX4. They cost little to meet early and a great deal to retrofit, and they're goals the Collective is working toward, and they haven't been audited.

- Honest labeling. The design labels synthetic data and demonstrations as such, forbids third-party trackers on health screens, and uses no real identifier in demonstrations.
- Access and identity. A unique identity for each person, groups, emergency access, automatic logoff and stronger sign-in options, with NIST's digital identity guidance as a reference.
- Audit. Reads as well as writes recorded in a tamper-evident trail, with scheduled review and testing planned.
- Supply chain. An SBOM for each build, dependency scanning with a fix schedule, integrity checks on bundled components, a secure-development process and, before the first public release, a vulnerability disclosure policy.
- Data rights and handling. Classification of each field, a retention schedule with deletion, right of access and an accounting of disclosures, a breach-assessment method, HIPAA de-identification practices for any data that leaves a customer, a privacy impact assessment for each new data flow, rules for minors and proxy access, and health reminders that carry no health detail.
- AI governance. Model cards and datasheets, a model change log, subgroup evaluation, adversarial testing of language-model features before each release, and prompt-injection defenses.
- Accessibility. The target is WCAG 2.2 AA, with voice-first alternatives; conformance hasn't been audited.
- Organization. One register of named, accountable roles and a written way of fitting pull-request-driven work to a regulated process.

Why it matters

A rule met late is met by rebuilding. The read log that wasn't in the data layer, the sensitivity class the data model had nowhere to hang, the basis view the screen was never laid out to show: each turns into a rewrite on the day the first clinic asks for it. Written into the design first, the same three cost a column, a field and a panel.

The order also decides who carries the risk. A clinician who signs an AI-drafted note answers for it, so the note has to show its basis before it asks for a signature. A

patient's record crosses systems the patient never sees, and the information-blocking and consent rules exist so that crossing stays theirs to control. A household's notes about a fall or a dose sit outside HIPAA and inside state consumer-health law until the person sends them to a clinic, and they deserve the care a chart gets, because with the person's say they become part of it.

For anyone building in this field, the change is in what gets settled before the stack: the data role, the stated purpose, the reader of the output and the user's state. Statutes keep moving and several are in court, so each of those answers carries a date, and the register holding them is read again before every gate. A system built that way can absorb a new rule. One built the other way meets each new rule as a migration.

What the Collective doesn't claim

- No device status. Whether any MARA function is or isn't a medical device hasn't been determined, and nothing here says any function is FDA cleared, approved, registered or compliant. How FDA would treat each function is an open legal question.
- No compliance. Nothing here says MAX4, MAX5, MARA or any part of them complies with HIPAA, any state law or any standard, or has been audited or certified.
- No program coverage. Nothing here says any feature is covered by, billable to, or supports claims to Medicare, Medicaid or any other government program (see Scope).
- A professional decides. MARA is designed so a clinician or other licensed reviewer makes each diagnosis and decision, and she's designed to organize information for that professional's review.
- Compliance is ongoing. Several dates above moved in the last month, and several statutes are in litigation.
- No legal review yet. This article hasn't been reviewed by a lawyer.

About the figures and the names in them. Figures 1 to 5 use invented data and describe no real person, clinic, plan or vendor. Figures 1, 2 and 5 were drawn for this

article; Figures 3 and 4 are mock-ups of the design. Each figure was checked visually for overlapping text; none has been audited for accessibility beyond the text alternatives supplied. Corrections can be sent to the MAX Research Collective through www.maxresearchcollective.com.

Sources

Primary sources for the legal points above, checked or re-checked as of 10 November 2026. Readers should consult the sources themselves rather than this list.

- HIPAA rules, 45 CFR Parts 160, 162 and 164: https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C
- HHS, Security Rule notice of proposed rulemaking, 90 FR 898 (6 January 2025): https://www.federalregister.gov/citation/90-FR-898
- FTC Act section 5, 15 USC 45; FTC Health Breach Notification Rule, 16 CFR Part 318: https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-318
- FTC Policy Statement on Deception (14 October 1983): https://search.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf
- 42 CFR Part 2: https://www.ecfr.gov/current/title-42/chapter-I/subchapter-A/part-2
- Section 1557 patient care decision support tools, 45 CFR 92.210: https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-A/part-92/subpart-C/section-92.210
- FD&C Act section 520(o)(1)(E), 21 USC 360j(o)(1)(E): https://www.law.cornell.edu/uscode/text/21/360j; FDA, Clinical Decision Support Software final guidance (29 January 2026) and General Wellness policy (revised 6 January 2026): https://www.fda.gov/regulatory-information/search-fda-guidance-documents
- FDA product classification, QIH (21 CFR 892.2050): https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfpcd/classification.cfm?id=QIH

- ONC information blocking, 45 CFR Part 171: https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-D/part-171; HTI-5 final rule, Federal Register document 2026-21943: https://www.federalregister.gov/d/2026-21943
- Colorado SB 26-189: https://leg.colorado.gov/bills/sb26-189; X.AI LLC v. Weiser (D. Colo. 1:26-cv-01515): https://www.troutmanprivacy.com/wp-content/uploads/sites/941/2026/04/US_DIS_COD_1_26cv1515_d8891528e364_MINUTE_ORDER_The_parties_Motion_ECF_No_22_is_GRANT.pdf
- Texas HB 149 (TRAIGA) and SB 1188: https://capitol.texas.gov/BillLookup/History.aspx?LegSess=89R&Bill=HB149
- Utah Code 13-77-103: https://le.utah.gov/xcode/Title13/Chapter77/C13-77-S103_2025050720250507.html
- Washington RCW 19.373 (My Health My Data Act): https://app.leg.wa.gov/RCW/default.aspx?cite=19.373
- Illinois Biometric Information Privacy Act, 740 ILCS 14: https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004
- Oregon SB 1546, companion chatbots (Oregon Laws 2026, chapter 85, effective 1 January 2027): https://www.oregonlegislature.gov/bills_laws/lawsstatutes/2026orLaw0085.pdf
- Oregon Consumer Privacy Act, ORS 646A.570 to 646A.589, and Oregon Consumer Information Protection Act, ORS 646A.600 to 646A.628: https://www.oregonlegislature.gov/bills_laws/ors/ors646A.html
- Portland City Code chapter 34.10: https://www.portland.gov/code/34/10
- NIST AI Risk Management Framework: https://www.nist.gov/itl/ai-risk-management-framework

Glossary

TERM	DEFINITION
510(k) and De Novo	FDA's two common premarket routes for a device. A 510(k) shows a device is substantially equivalent to one already on the market; De Novo classifies a new, lower-risk type.
ADT feed	admission, discharge and transfer messages a hospital system sends as patients move.
Automation bias	the habit of trusting a machine's output too readily, which is why the design adds friction to sign-off.
BAA (business associate agreement)	the contract HIPAA requires between a covered entity and a vendor handling protected health information for it.
BIPA	Illinois's Biometric Information Privacy Act, which requires a written release before collecting biometric identifiers and carries a private right of action.
Business associate	a vendor that handles protected health information for a covered entity.
C-CDA	Consolidated Clinical Document Architecture, the HL7 standard for clinical documents such as visit summaries.
CDS (clinical decision support)	software that gives a clinician information to weigh; some of it is outside the FDA device definition if it meets all four statutory criteria.
CMS	the Centers for Medicare & Medicaid Services, the federal agency whose interoperability and prior-authorization rules bind payers.
Covered entity	under HIPAA, a health plan, a health care clearinghouse, or a provider that transmits health information electronically in standard transactions.

TERM	DEFINITION
De-identification	under 45 CFR 164.514, either Expert Determination by a qualified expert, or Safe Harbor, which removes the eighteen kinds of identifiers HIPAA lists with no actual knowledge that what remains could identify a person.
DICOM	Digital Imaging and Communications in Medicine, the standard for medical images and their headers.
EHR	electronic health record, the clinical system a provider keeps a patient's chart in.
FHIR	Fast Healthcare Interoperability Resources, HL7's web standard for exchanging health data; US Core sets its US baseline and SMART on FHIR handles app launch and sign-in.
HIPAA	the Health Insurance Portability and Accountability Act, whose rules govern protected health information held by covered entities and business associates.
HITECH	the 2009 act that extended HIPAA's duties and penalties to business associates and added breach notification.
HL7	Health Level Seven, the standards body behind HL7 v2 messages, C-CDA and FHIR.
Information blocking	unreasonably interfering with access to, exchange of or use of electronic health information, barred by ONC's rules subject to defined exceptions.
IRB	an institutional review board, which can approve research use of health data or waive the need for each person's authorization.
Knowledge graph	a store that records things (patients, visits, findings) and the links between them, so related facts can be followed.
ONC	the Office of the National Coordinator for Health IT, which runs health IT certification and the information-blocking rules.

TERM	DEFINITION
Part 2	42 CFR Part 2, the federal rule on substance-use-disorder treatment records, stricter than HIPAA on consent and redisclosure.
PCCP	a predetermined change control plan, the way a device maker agrees in advance with FDA how an AI model will be updated.
PHI	protected health information, the individually identifiable health information HIPAA governs.
Product code	FDA's three-letter label for a device type, which ties it to a classification regulation.
QMSR	FDA's Quality Management System Regulation, aligned with ISO 13485, the quality system a device maker runs.
Resident	the Collective's name for an assistant that lives on one machine; MAX4 is the resident in progress, MAX5 the planned consumer release and MARA the planned healthcare version.
SBOM	a software bill of materials, the list of every component in a build.
SOC 2 Type II	an auditor's report on a company's controls over a period of time, which hospital buyers often ask for.
Synthetic data	invented records that describe no real person.
TEFCA	the Trusted Exchange Framework and Common Agreement, the federal framework for nationwide health information networks.
Trust ladder	the graded levels of independence a resident's abilities earn, from proposing to acting; the design has no autonomous rung for clinical decisions or claims.
USCDI	the United States Core Data for Interoperability, the federal baseline set of data elements systems must be able to exchange.
Vector embedding	a numeric fingerprint of a note or result that lets similar records be found together.

TERM	DEFINITION
X12	the standard behind HIPAA's adopted electronic transactions, such as eligibility checks (270/271).

HEALTHCARE ART-HLC-024

// ABOUT THE AUTHOR

Jason Newell leads organizations and people in technology, and is a researcher, deep technologist and builder — from a CRAY to agentic AI. He founded MAX Research Collective to build AI for regulated industries that runs where its owner has control, with healthcare as its strongest focus. About Jason → Connect on LinkedIn → ORCID →