// ARTICLE · PUBLISHED 24 OCTOBER 2026

Patient Records and AI Agents: The Patient Holds the Keys

Patients are already moving their records into AI tools, and the route they take decides whether anyone can later check what the AI read

Jason Newell · MAX Research Collective · Article ART-HLC-015 · Published 24 October 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/patient-records-and-ai-agents.html
Cite as: Newell, J. (2026). Patient Records and AI Agents: The Patient Holds the Keys. MAX Research Collective, ART-HLC-015. https://www.maxresearchcollective.com/articles/patient-records-and-ai-agents.html

The record leaves through the patient

Patients are handing their medical records to AI. The route they use decides who can see what happened afterwards. Most copy the record into a general chatbot. A few designs keep the record in a store the patient controls and let an AI agent in for one named purpose, with a receipt for every step. That second route is slower and harder to build; it's also the only one in which a clinician can check what the agent actually read.

A federal award announced on 6 October 2026 pays for an open version of that second route, built on a data protocol called Solid. The plan is small, open and unproven. MARA, the Medical Agentic Resident Assistant this project is designing, has already moved toward it. And the evidence that patients won't wait comes from one health system's bill for data requests.

Patients are already doing it

At Advocate Health, patients linking their MyChart accounts to ChatGPT rose 7,000% between July and August 2026. MyChart is the patient portal that comes with the

Epic electronic health record, and the figure comes from Dr. Bobbie Byrne, Advocate's chief information officer, speaking to Becker's Hospital Review. Advocate sees the growth as application programming interface (API) calls against its own Epic system, since every linked account and every request reaches back into the record. "This is completely driven by individual patient actions," she said.

The figure has limits. Becker's gives no starting count, so 7,000% could mean a few hundred patients or a great many. It doesn't say whether a patient who linked twice was counted twice either.

The direction is clear all the same. Records are leaving through the patient, one account at a time, and the health system finds out from its own API bill.

Patients can do this because the law makes the record theirs to get. The federal information-blocking rule, 45 CFR 171, covers health IT developers, health information networks and providers. It bars them from practices likely to "interfere with access, exchange, or use of electronic health information," unless the law requires the practice or an exception applies. The Centers for Medicare & Medicaid Services (CMS) push from the payer side. Under its Interoperability and Prior Authorization final rule, CMS-0057-F, affected payers meet some provisions from 1 January 2026; most of the API requirements follow on 1 January 2027. Both rules push records toward patients through standard interfaces. Once a patient holds a record, a chatbot is one paste away.

Two ways to give an AI your record

The two routes start from the same record and end in very different places.

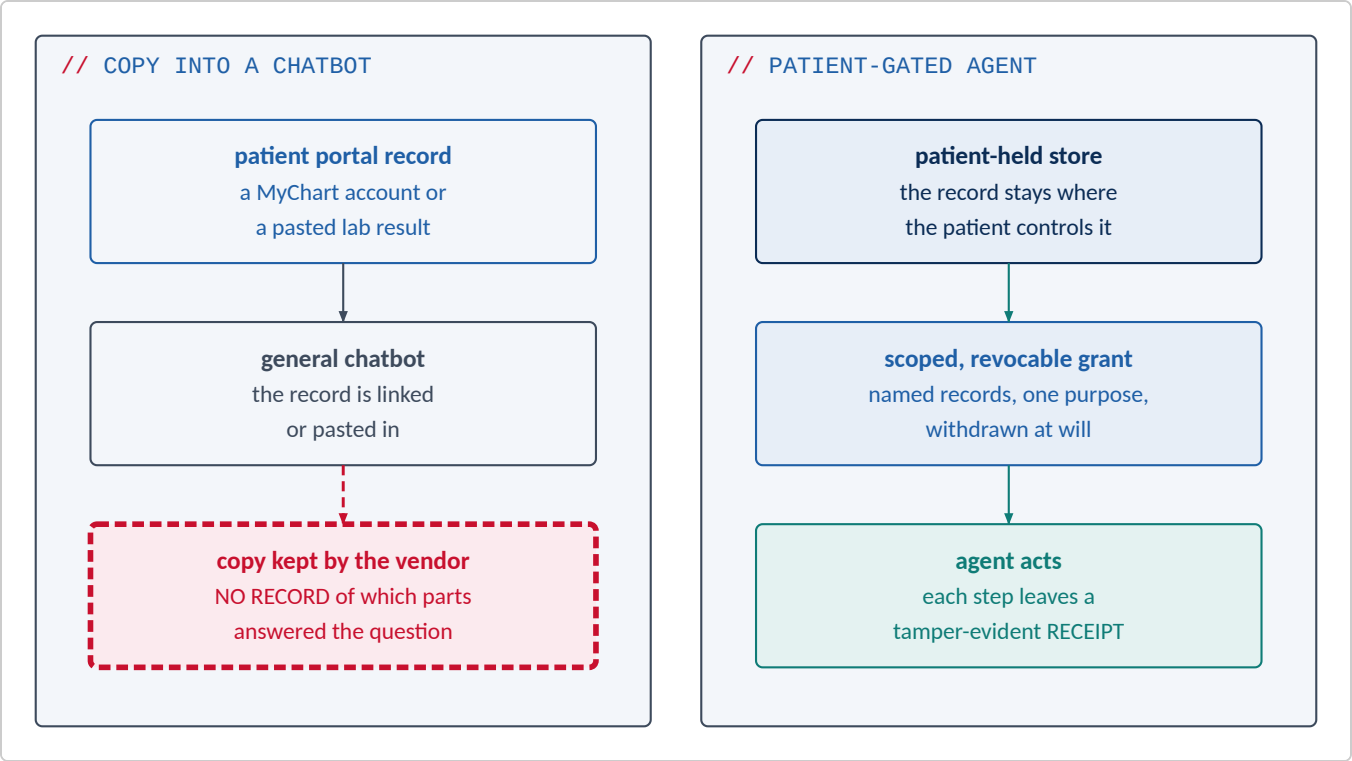


Figure 1. Both routes start with the patient's record, and only the right-hand one leaves a receipt for each step the agent takes.

The first route copies the record into a chatbot. The patient links a portal account or pastes a result into a general assistant. It's easy. It's often useful, too, since a plain-language reading of a lab value is worth having at eleven at night. Once the copy leaves, though, the patient has little say over where it goes next. There's usually no record of which parts of the history the assistant used to reach its answer, so a clinician can't check the reasoning against the source. HIPAA, the federal health privacy law, generally doesn't reach a consumer chatbot. The protections a patient expects inside a hospital may not travel with the data.

The second route uses a patient-gated agent. The record stays put. The patient grants an agent access to named parts of it for one purpose, can withdraw that grant whenever they like, and gets a written account of every action the agent took, kept in a form nobody can quietly alter afterwards.

That costs something (setup, keys to manage, a slower first answer). What it buys is accountability.

What MedStar is building

On 6 October 2026 the Office of the National Coordinator for Health IT (ONC), the federal office that sets health IT policy, announced this year's awards under LEAP in Health IT, its grant programme for projects it wants built. The round has two awards totalling $1.5 million: one to the MedStar Health Research Institute, and one to the Regenstrief Institute for laboratory terminology. ONC didn't give the split.

MedStar's project is called "Sovereign Execution: Vigilant, Gated and Verifiable Agentic Care." Its goal, in ONC's description, is AI that coordinates care while the patient keeps control of the AI. The deliverable is the Sovereign Execution Bridge, a piece of middleware for long clinical follow-ups. Middleware is software that sits between systems and passes work along. The bridge has three named parts.

- Durable, long-running processes keep a task alive across weeks, since a referral or a repeat test can take that long.
- Patient-gated data pods built on the Solid protocol hold the record where the patient decides who reads it.
- Cryptographically verifiable AI routing with tamper-evident certificates gives every step a record that shows any later change.

ONC calls the bridge fully open source and names no licence. I found no published code on 21 October and no results. It's a plan.

What Solid is

Solid is a set of specifications for keeping data where its owner controls it. Applications read that data only with permission. The W3C Solid Community Group writes the specifications, and the pieces are few. A WebID, a web address that returns a profile, names each person or application. Data sits in a storage with one owner, usually called a pod. A server must support Web Access Control or Access Control Policy to decide who reads what, and the recommended sign-in is Solid-OIDC, a version of the OpenID Connect login standard.

Two limits matter for a clinic. The protocol is at version 0.11.0, a draft dated 12 May 2024, and it says of itself that it "is not a W3C Standard nor is it on the W3C

Standards Track.” Solid is also a general data protocol. Hospitals exchange records in clinical formats such as HL7 FHIR (Fast Healthcare Interoperability Resources), and a health pod would keep those formats. Solid’s job is narrower: deciding who may open them.

Sovereign by region, sovereign by patient

”Sovereignty” means something else in Europe. Tandem Health, a Swedish clinical-AI company, offers ”Sovereign Health,” which ”keeps both patient data storage and AI processing on European-owned cloud infrastructure.” That’s the Healthcare AI Guy newsletter’s wording of 20 October, and Tandem’s own product page bears it out: the service runs on Scaleway, a European cloud provider, and Tandem holds the encryption keys. The company raised a $100 million Series B in September 2026, led by the Scaleup Europe Fund, and reports about 10,000 care organisations in 14 European markets.

That kind of sovereignty is about the country or the region. It answers whose laws govern the data. Solid answers a smaller and sharper question, which is who may open a given record today.

Where MARA sits

MARA is a design for a clinical assistant. She gathers a patient’s record, checks it and recommends, and a person makes every decision. She’s a resident, living on hardware in the clinic or the home rather than visiting from a remote service. That already puts her nearer the gated route, and the MedStar design has moved her three steps further.

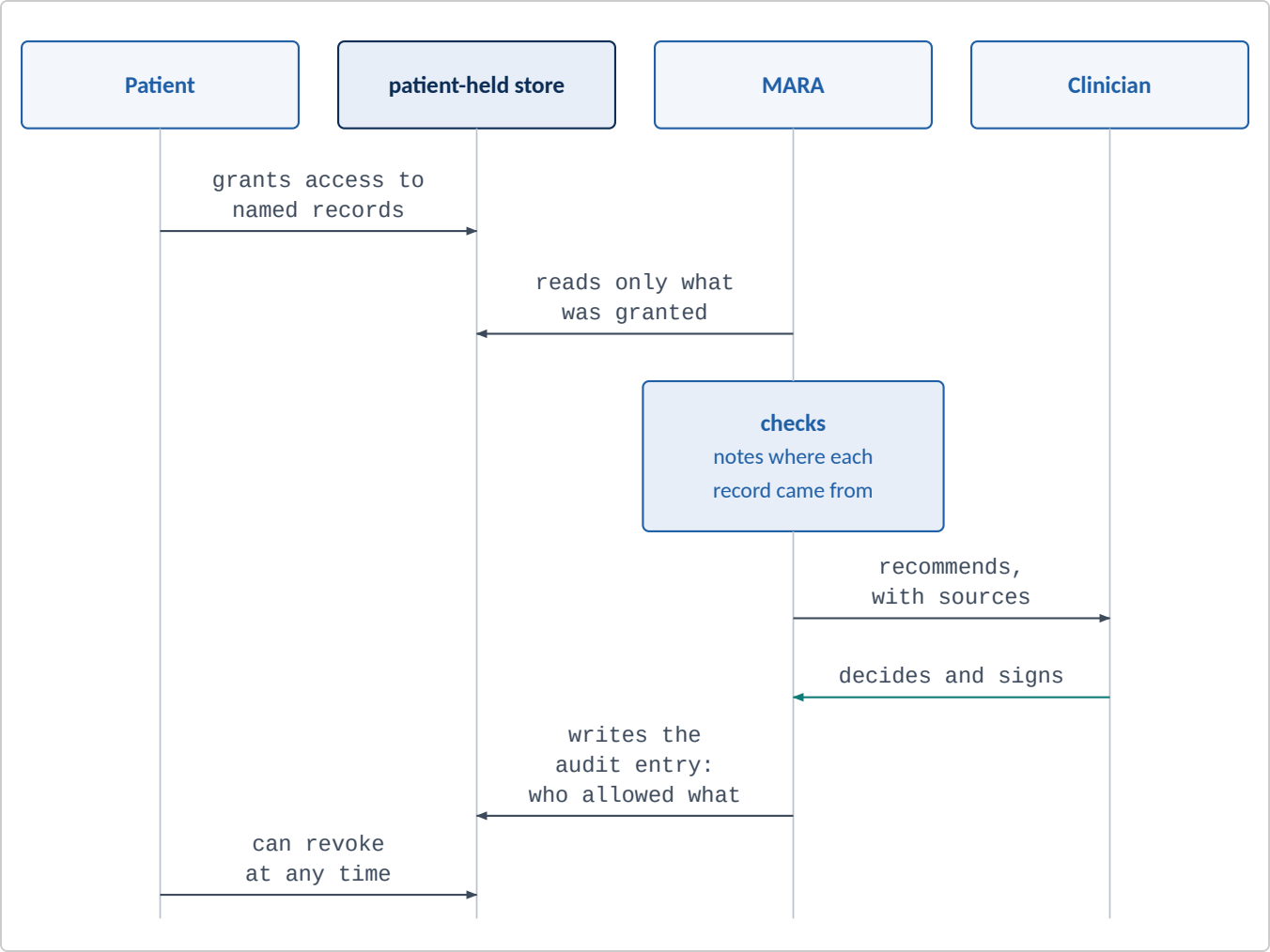


Figure 2. Read down the page: the patient grants, MARA reads only what was granted, a clinician signs, and the audit entry lands back in the patient's store.

1. Patient-gated stores are now a candidate. MARA's design lists Solid-style pods as an option for the patient's own store, beside the clinic's record.
2. Every record a patient brings carries its provenance. A MyChart export is labelled as patient-supplied, with its date. MARA never treats it as the hospital's own copy.
3. The audit log is tamper-evident. Each entry is chained to the one before it, so changing one breaks the chain. Every entry names who allowed the action.

None of this is proven. MARA hasn't been built past an early demo, and the first test of these behaviours runs in MAX4, the desktop system she's being developed from. The gated route has costs of its own, too — the worst is a patient locked out of their own store.

What nobody knows yet

Four questions are open, and the answers will decide whether the gated route is used or only admired.

- The size of the shift is unknown. The Advocate figure has no baseline. A survey of 1,000 recent surgery and hospital patients, in which 42% said they had used AI instead of a doctor, run by PayZen, a medical-bill payment company, is known only from the newsletter.
- The release is unknown. Nobody knows yet whether MedStar's bridge ships, or under which licence. Patients may not keep pods at all; earlier personal health record efforts struggled to find users.
- The fit with clinical formats is untested. Whether Solid's access controls hold up for clinical data, and how they combine with FHIR, hasn't been shown in practice.
- The legal standing of the agent is unsettled. Courts and regulators haven't said whether an agent acting under a patient's grant is the patient's tool, the provider's, or neither.

Why it matters

A record that leaves as a copy leaves its evidence with the vendor. A clinician handed the chatbot's answer has nothing to check it against. A patient who regrets the paste has nothing to revoke.

The gated route moves that evidence back to the person the record describes, and that's the condition under which a clinician can trust an AI's reading at all. Advocate learned what its patients were doing from an API bill. The next health system could learn it from a receipt the patient chose to share.

Sources

- Office of the National Coordinator for Health IT. "HHS announces 2026 LEAP in Health IT awardees to accelerate the use of agentic AI in clinical care and close gaps in laboratory interoperability." 6 October 2026. https://healthit.gov/news/hhs-announces-2026-leap-in-health-it-awardees-to-

accelerate-the-use-of-agentic-ai-in-clinical-care-and-close-gaps-in-laboratory-interoperability/

- W3C Solid Community Group. Solid Protocol, version 0.11.0, draft of 12 May 2024. https://solidproject.org/TR/protocol
- 45 CFR 171.103, Information blocking, via the Legal Information Institute. https://www.law.cornell.edu/cfr/text/45/171.103
- Centers for Medicare & Medicaid Services. CMS Interoperability and Prior Authorization Final Rule (CMS-0057-F). https://www.cms.gov/cms-interoperability-and-prior-authorization-final-rule-cms-0057-f
- Becker's Hospital Review. "Patients linking MyChart to ChatGPT jumped 7,000% at Advocate: who pays?" Opened 21 October 2026. https://www.beckershospitalreview.com/healthcare-information-technology/ai/patients-linking-mychart-to-chatgpt-jumped-7000-at-advocate-who-pays/
- Healthcare AI Guy Weekly, 20 October 2026, the only source for the PayZen survey. https://www.healthcareaiguy.com/p/healthcare-ai-guy-weekly-10-20
- Tandem Health. "Sovereign Health." Opened 21 October 2026. https://tandemhealth.ai/sovereign-health
- HLTH. "Tandem Health raises $100M to expand clinical AI across Europe." 15 September 2026. https://hlth.com/insights/news/tandem-health-raises-100m-to-expand-clinical-ai-across-europe

Glossary

TERM	DEFINITION
API (application programming interface)	the agreed way one program asks another for data. Patient apps and chatbots reach a health record through one, which is how Advocate counted the links.
FHIR (Fast Healthcare Interoperability Resources)	the HL7 standard for exchanging health records between systems. A health pod would still store records in it.
Information blocking	a practice likely to interfere with access to, exchange of or use of electronic health information. It's barred for developers, networks and providers unless an exception applies, which is what lets patients get their records.
LEAP in Health IT	ONC's award programme for health IT projects. Its 2026 round funds MedStar's patient-gated agent work.
MARA (Medical Agentic Resident Assistant)	this project's design for a clinical assistant that recommends while a person decides. She's the reason the gated route matters here.
MAX4	the desktop generation of the MAX AI resident, from October 2026 on, and the system MARA is being developed from.
Middleware	software that sits between systems and passes work along between them. The Sovereign Execution Bridge is middleware for clinical follow-ups.
MyChart	the patient portal attached to the Epic health record. It's the account Advocate's patients linked to ChatGPT.
Pod	the usual name for a storage in Solid, a data store with one owner. It's where a patient-gated record would live.
Provenance	a record of where a piece of data came from and when. MARA labels a patient-supplied export with its provenance so nobody mistakes it for

TERM	DEFINITION
	the hospital's copy.
Solid	a set of open specifications for data stores that their owners control, written by a W3C community group. MedStar's project builds on it.
Tamper-evident	built so that any change after the fact can be detected. An audit log of that kind lets a patient or a clinician trust what an agent's record says.
WebID	a web address that identifies a person or an application in Solid. It's how a pod knows who is asking.

HEALTHCARE ART-HLC-015

// 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 →