



The Light Collective's Response to CMS/ASTP RFI on Health IT Modernization

Table of Contents

Table of Contents	1
Signed By:	3
The Light Collective’s Response to CMS/ASTP RFI on Health IT Modernization	4
Introduction	4
I. Duty To Patient Outcomes First; Free From Conflict of Interest	4
II. Community Data Stewardship & Peer Navigation	5
III. The Need for Trusted, Patient-Led Community Infrastructure & Services	6
IV. AI and Patient-Generated Data: Risk and Opportunity	7
VI. Final Considerations: Governance and Federal Alignment	10
APPENDIX	11
1. RFI Questions / Comments	11
PC-1. What health management or care navigation apps would help you understand and manage your (or your loved ones') health needs, as well as the actions you should take?	11
VB-1. Incentives for APMs to Adopt Digital Health Navigation Tools	12
VB-5 to VB-7: Certification and Compliance Enhancements	14
VB-8. Supplementing CEHRT Through HHS Policy	15
VB-10. CEHRT Flexibility for Advanced APMs	15
2. Suggested Resources: Civic Data Trusts as Federated Infrastructure for Patient-Partnered Innovation	15
Overview	15
A. Patient-Governance Sandboxes For Health Tech	16
1. Federated Patient Infrastructure	16
2. Civic Data Trusts	16
3. Patient Outcomes and Evaluation Metrics	17
4. Key Scholarly Articles on Data Trusts and Data Loyalty in Health (2017–2025)	18
A. Data Trusts and Health Data Stewardship	18
B. Data Loyalty and Fiduciary Duties for Health Data	19



Centers for Medicare & Medicaid Services (CMS)
U.S. Department of Health and Human Services
Washington, DC 20201

RE: RFI on Medicare Technology Modernization

Dear CMS and ASTP Leadership,

Thank you for the opportunity to provide comments through your RFI on [The Health Technology Ecosystem](#).

As a coalition of patient advocates, community-based organizations, and clinical experts, we welcome this opportunity to shape a vision for fair, ethical, and effective digital health transformation.

Our comments reflect the lived experience and expertise of patient communities who rely on digital tools to access care, connect with one another, and navigate complex health systems—often in the absence of accessible, trusted, and safe alternatives. We have engaged directly in national efforts to co-create standards for ethical AI in healthcare, partnered with clinical and public sector institutions to prototype digitally enabled care navigation, and supported coalitions of patients and caregivers impacted by privacy harms and data misuse.

Our collective input focuses on core themes:

1. **Duty to Patient Outcomes First:** Patients should not have to rely on surveillance-based social media or monopolistic technology vendors to steward their health data or coordinate care. We therefore outline concrete models for [fiduciary loyalty](#) to patient interests. We advocate for federated digital tools that support independent governance and shared accountability. We hope for opportunities to develop patient data governance sandboxes (see Appendix, Section 3)
2. **Care Navigation as Health Infrastructure:** Social and peer support—especially for patients navigating chronic, rare, or stigmatized conditions—is an essential part of the care continuum. We urge CMS to support billing models for digital infrastructure that replaces extractive platforms with trusted, community-moderated alternatives.
3. **Ethical AI Adoption:** Drawing on the [Patient AI Rights Initiative](#) and cross-sector partnerships, we uniquely propose that health technology should hold independent duty to patient communities. Simply anonymizing data and implementing privacy policies is not adequate to protect the integrity, security, and privacy of health technology in an age of AI. Patients must have a voice in how these technologies are designed, developed, and deployed.

4. **CMS Incentives & Reflect Real-World Fairness:** We provide recommendations on certification, data interoperability, and Alternative Payment Model (APM)-related incentives that prioritize usability, accessibility, and community-level impact, especially in rural and under-resourced settings.

We believe this modernization effort presents a rare and powerful opportunity to realign the nation's health technology investments with values of justice, trust, and dignity. We are eager to work alongside CMS to build infrastructure that puts patients at the center—not just as users or data sources, but as co-designers and stewards of our shared digital future. To quote an important advocate who spoke about her experience over a decade ago, “*We are the patients and we need to be heard.*”

Signed By:

Andrea Downing
Co-Founder & Board President
[The Light Collective](#)

Valencia Robinson
Co-Founder | Community Outreach
[The Light Collective](#)

Erica Olenski
Vice President, FINN Partners
Founder, [August's Artists](#)

Sneha Dave
Founder & Executive Director
[Generation Patient](#)

Ysabel Duron
Founder/ Executive Director
[The Latino Cancer Institute](#)

David M. White
Board of Directors
[The Light Collective](#)

Mary K Gurney, PhD
Professor
Midwestern University College of Pharmacy

The Light Collective's Response to CMS/ASTP RFI on Health IT Modernization

Introduction

[The Light Collective](#) (TLC) is a nonprofit organization working to advance the rights, interests, and voices of patient communities in health technology. We focus on co-developing patient-led infrastructures to ensure community-governed, safe, and inclusive spaces for health data exchange and peer support. We outline several key recommendations and responses to CMS below in key themes. Our Appendix provides comments to specific questions in the RFI.

I. Duty To Patient Outcomes First; Free From Conflict of Interest

As CMS considers expanding support for digital navigation, social support tools, and care coordination infrastructure, we urge the agency to include **clear conflict of interest protections** to ensure that vendors entrusted with sensitive patient engagement responsibilities are aligned with the ethical values of public health—not commercial exploitation.

Specifically, any entity or vendor seeking reimbursement under Medicare billing codes for care navigation, social support, or patient engagement should be required to demonstrate that they:

- Do not collect, repurpose, or monetize sensitive patient data for non-health-related uses, especially in ways that could harm vulnerable populations through targeted advertising, or deploy [banned surveillance technologies](#).
- Are not simultaneously engaged in activities that conflict with the interests of patient communities—such as data brokerage, credit scoring, criminal background aggregation, voter profiling, or business models that rely on pharmaceutical advertising in ways that worsen [cyber harms in digital health](#).
- Maintain clear and independent governance structures that prevent the blending of health engagement services with surveillance, targeted marketing, or predictive risk scoring unrelated to care.

A vendor that, for example, profits from gathering financial histories, delivering targeted drug ads, criminal records, or conducting voter data analytics should not be eligible for reimbursement under Medicare billing codes intended to strengthen social support or peer navigation. These activities undermine patient trust, [undermine national security](#), and introduce systemic risks into programs designed by CMS to improve equitable care.

We recommend that CMS develop a vendor certification framework—to prioritize patient-aligned, non-conflicted organizations are authorized to deliver reimbursable support services in Medicare. CMS could build upon existing tools such as the ONC Health IT

Certification Program for EHRs provides a strong precedent, including developer attestation, real-world testing, and compliance reporting.

II. Community Data Stewardship & Peer Navigation

The Challenge: Patient communities are often left to rely on fragmented, unregulated health technology for social support, peer navigation, and care coordination—tools that exist outside the formal healthcare system and are rarely evaluated for safety, quality, or fairness for patients.

These resources fill critical gaps in care, especially for people managing rare, chronic, or stigmatized conditions, yet they are not integrated into clinical workflows or supported by sustainable reimbursement mechanisms. As a result, patients are frequently exposed to misinformation, emotional harm, or exploitative data practices, with no formal oversight or accountability. Without CMS recognition or financial support for community-developed digital tools that provide safe, moderated, and culturally relevant peer support, the healthcare system misses a key opportunity to strengthen outcomes and trust across the patient journey. These tools must be vetted, integrated, and reimbursed as legitimate components of coordinated, value-based care.

Opportunity for CMS: We urge CMS to use its Innovation Models and Demonstrations, via the Center for Medicare and Medicaid Innovation (CMMI), as a primary pathway to test and validate Federated Patient Infrastructure and Civic Data Trusts—patient- and community-led data ecosystems that are interoperable, privacy-preserving, and collectively governed.

This approach would align with CMMI's mission to test alternative care models that improve quality and reduce costs, while empowering Medicare beneficiaries to safely engage with digital health tools outside of exploitative commercial platforms.

Policy Recommendations:

- **Support Federated Data Models Through Innovation Pilots:** Create or amend existing CMMI demonstration models (such as [ACO REACH](#) or new patient-focused models) to include funding and evaluation support for **interoperable, community-controlled data systems**. These systems should prioritize **contextual consent**, data minimization, and participatory governance frameworks modeled on public trust and shared accountability.
- **Embed Patient-Centered Data Stewardship into APM Infrastructure:** Require or incentivize [Alternative Payment Models \(APMs\)](#) to partner with nonprofit technology collaboratives and patient-led coalitions to build secure, standards-based infrastructure for shared data stewardship. This includes tools for transparent data access, digital identity management, and AI risk flagging.
- **Leverage the CMMI Evaluation Framework:** Use existing CMMI evaluation and learning frameworks to rigorously assess outcomes such as patient trust, digital safety, access, and system-level efficiency when civic data trusts or community-led digital tools are implemented alongside or in place of commercial platforms.

III. The Need for Trusted, Patient-Led Community Infrastructure & Services

Challenge:

Patient communities have long relied on commercial social media to find one another, share their personal stories, seek knowledge, and access [peer health advice](#) to fill unmet needs in healthcare. Unfortunately online spaces are full of hackers, marketers, and scammers to take advantage of people going through the trauma of a medical diagnosis. Social media often fills gaps left by formal care systems, particularly for people navigating rare, chronic, or stigmatized conditions. However, the dependence on social platforms—many of which are not designed with health integrity or safety in mind—comes at a cost. Misinformation, lack of moderation, algorithmic targeting, and exposure to health surveillance and data harvesting have created a risky environment for vulnerable populations seeking trusted guidance online.

In our 2024 community-led study, [Tangled in the Web](#), we learned that 73% of respondents reported participating in online support groups, with the vast majority accessing them through general-purpose platforms where medical misinformation proliferates. A significant share expressed concern about privacy violations and data misuse, while 74% were moderately to extremely concerned about their security as well as the unauthorized sharing of their health data.

What's Needed:

Federal health IT modernization efforts must support the development of **community-driven digital infrastructure** that is governed, moderated, and co-designed by the patient communities themselves. This infrastructure should not only support innovation, but help patient communities collectively to build market power, and evidence in a data sharing economy has been built “about us without us.”

This shift in focus for CMS includes building technology that honors the digital rights of patients, aligns with principles of collective governance, and provides alternatives to social media environments where safety, privacy, and trust are compromised.

Policy Recommendations:

In this section we offer specific ideas, building upon past programs. Care navigation needs supported “patient community partnership” to guide patients through complex treatment pathways, improve adherence, and help drive down avoidable costs like ED visits and readmissions. One initial step forward has been CMS’s creation of G-codes for [Principal Illness Navigation \(PIN\)](#) signaled strong support for care navigation.

But to realize the vision for PIn Services, we need to recognize that there are hurdles. RVUs are the building blocks of Medicare’s physician fee-schedule, and drive new services that can support unmet needs for care navigation. However in practice the low RVUs and narrow

coverage for PIN Services have hindered wider adoption. To unlock the full value of PIN in cancer care and ensure financial sustainability, CMS should consider making these codes more feasible to implement. Here are specific recommendations:

- **Raise G-code Rates:** As an example in cancer care, hospital oncologists state the barrier for PIN services is that RVUs don't cover the \$70/hr cost of hiring and running a single navigator. A potential solution is to increase G0023/G0024 to at least \$70/hr, and index the rate for complexity of an illness.
- **Require Payer Parity:** The barrier is that PIN G-codes are Medicare-only; which means commercial and Medicaid plans often exclude or underpay. A potential solution is to mandate all payers reimburse G0023–G0146 at Medicare rates.
- **Carve-Out in Bundles:** A barrier is that capitation models subsume navigation into lump sums. A potential solution is to allow discrete PIN add-ons or carve-outs inside oncology APM bundles.
- **Offset Tech Build-Out:** A barrier for adoption is the lack of EHR templates, validate peer support solutions and care-coordination platforms that require upfront investment. A potential solution is for CMS to help incentivize a “digital navigation” payment to cover IT setup and licensing.
- **Pilot Community Platforms:** A hurdle for health systems is too standardized, secure referral network to social supports. A key solution we recommend is to fund patient-governed platform pilots with built-in consent, transparency, and cyber-hygiene co-designed by the community.
- **Certify the Workforce:** A hurdle in adoption is inconsistent training and credentialing for care navigators and peer specialists. It would be helpful to **establish, fund, and support a CMS-endorsed Navigator certification** and apprenticeship pathways directly for patient advocates with lived experience of a chronic health condition.
- **Tie to Outcomes:** Without data on reduced hospitalizations or ED visits, PIN looks like overhead. Here we hope CMS would link shared-savings compensation to patient-reported navigation metrics in oncology APMs.
- **Protect Patient Data:** A risk that digital tools may create privacy and security issues, especially if vendors “re-monetize” or broker patient data. We strongly recommend CMS **ban billing for data brokering** and enforce BAAs locking in patient-defined privacy, data minimization, and governance standards. For example, CMS could specify that providers using [banned tracking technologies](#) cannot be compensated for services.

IV. AI and Patient-Generated Data: Risk and Opportunity

Patients are not anti-technology but our communities have deep and justified mistrust that comes from years of mishandling our health data. For example in our own community-led study, 81% of respondents in our research support AI for use in disease screening and diagnosis. But 78% worry about misuse of our health data without consent, and 76% cite lack of transparency as a major concern ([SEE: Tangled In The Web 2024](#)). Current commercial health IT platforms

rarely align with these expectations, leaving patients to sign away their rights in privacy policies that work against our interests.

Recommendations To Co-Design The Future of AI:

- **Participatory AI Models:** Several national initiatives have taken a “top-down” approach to developing AI standards to date. In contrast we advocate that CMS support learning network programs where clinical sites and patient communities co-design AI features that interact with their data. CMS could leverage this to define what “AI readiness” looks like in community-led settings, rather than just institutional or commercial contexts.
- **Ethical AI Guidance:** In 2024 we developed a position statement with nationally recognized patient advocates to inform the goals, priorities, and unmet needs of patients. We hope CMS will review our guidance from [The Patient AI Rights Initiative](#).

Why This Matters for Patient Outcomes:

Patient communities are already navigating environments where their data is extracted without consent, commodified, and weaponized through targeted advertising and discriminatory algorithms.

A future where private / incumbent technology firms control or build the backbone of Medicare’s technology stack would deepen mistrust, especially among historically marginalized and medically vulnerable populations. These firms operate with proprietary codebases, minimal transparency, and little to no opportunity for community governance or redress.

Policy Recommendations:

- **Mandate Open Standards and Interoperability:** CMS must ensure that any technology adopted under this modernization agenda is built on open-source or open standards-based infrastructure, with auditability and community oversight built in from day one.
- **Vendor Restrictions:** CMS should explicitly restrict vendors from gaining exclusive control over Medicare patient data systems or architectures, especially those with existing dominance in government surveillance or defense contracting sectors. We urge CMS to exclude from its procurements any solution provider or vendor with a documented history of opaque data-sharing practices, or insufficient safeguards around re-identification risk. To protect patient trust, CMS should refrain from funding platforms developed by organizations that have partnered with intelligence or law-enforcement agencies in ways that conflict with healthcare privacy and patient-centered principles.
- **Diversify Technology Partners:** Create incentive pathways for nonprofit, community-governed, and patient-led technology solutions that prioritize data minimization, community control, and digital justice.

Why Now: The speed of this modernization push is notable—but speed should not come at the expense of accountability. We believe the testing and development of AI standards only works in

practice if the digital infrastructure is grounded in trust, participatory design, governed by the communities it serves, and protected from the extractive logic of monopolistic firms.

V. No Aggregation Without Representation: AI and Data Governance Standards

Challenge: A significant challenge in the current digital health ecosystem is the widespread deployment of AI-driven tools that operate with limited transparency, inadequate accountability mechanisms, and minimal patient input.

Despite growing adoption, patients remain deeply concerned about how AI systems influence health decisions—particularly when they lack clear explanations or fail to disclose their methods of data use. A 2024 study published in *JAMA Network Open* found that while most Americans support the use of AI in health care when it improves efficiency or expands access, **over 60% are uncomfortable with AI making diagnostic or treatment decisions without human oversight**, and **over 70% are concerned about potential bias and data misuse** in AI algorithms.

The study also found significant variation in trust based on race, age, and education, with Black and Latino respondents expressing higher levels of concern about AI safety and surveillance. These findings underscore a systemic trust gap and a critical need for patient-governed frameworks that prioritize transparency, consent, and fairness. Without embedding ethical standards into the development and deployment of AI tools, their use in value-based care could deepen existing disparities and undermine public confidence in digital health innovation.

Actionable Recommendation: CMS should implement clear certification standards for ethical AI and data governance within its Innovation Models that creates patient representation and voting rights.

To ensure that AI integration in Medicare is ethical, equitable, and aligned with patient needs, implementation should prioritize independent governance mechanisms with a strong focus on patient outcomes, as outlined in the [Patient AI Rights Initiative](#).

We might explore supporting ways to complement the ONC Health IT Certification Program by introducing new criteria that assess not only technical interoperability, but also patient evaluation, governance, and voting rights. CMS should also require that any federally supported digital health platforms—particularly those engaging in predictive analytics or care navigation—operate under **patient-aligned governance structures**, such as advisory boards led by patient advocates or co-ownership models with nonprofit intermediaries. To prevent conflicts of interest, vendors must complete a standardized attestation process disclosing any

data monetization practices or affiliations that could misalign with public health goals. These mechanisms, collectively, ensure that AI tools are not only explainable but also **accountable to the people they serve**. The intended outcome is a digital ecosystem where Medicare beneficiaries can trust how their data is used, how decisions are made, and who is ultimately responsible for ensuring safety, accuracy, and equitable benefit.

VI. Final Considerations: Governance and Federal Alignment

The long-term modernization of Medicare must move beyond digitization and embrace **ethical infrastructure** that:

- CMS can help communities move beyond the illusion of control over our rights, privacy, security, and safety in health technology.
- Help patients reduce systemic dependency on for-profit surveillance platforms where individuals navigating care are seeking knowledge along their health journeys.
- Explore shared helping patient communities to build market power within accountable, independent noncommercial trusts to govern shared health information.
- Recognizes patient peer support networks as core health infrastructure deserving direct investment.

CMS and ASTP have a critical window of opportunity to signal that safety, trust, and governance are as important as innovation. The Light Collective urges the agencies to respond not only to what can be built quickly, but to what can last—digital tools built *with* patients, *for* communities, and *by* trusted civic organizations.

APPENDIX

In response to the CMS and ASTP Request for Information on Medicare technology modernization, we are submitting the following detailed comments addressing specific questions outlined in the appendix, particularly under the sections titled **1. Digital Health Adoption** and **2. Compliance and Certification**. Our responses reflect lived experience, policy expertise, and insights from multi-stakeholder collaborations focused on patient data governance, digital access, and ethical health innovation. We offer actionable recommendations that draw on community-led models and public interest frameworks—including those developed through national initiatives like the Patient AI Rights Initiative—to help CMS design technology strategies that are effective, trustworthy, and rooted in the real-world needs of patients.

1. RFI Questions / Comments

PC-1. What health management or care navigation apps would help you understand and manage your (or your loved ones') health needs, as well as the actions you should take?

Many Medicare beneficiaries rely on digital tools—often developed by **consumer technology companies that are not covered by HIPAA**—for health management, care navigation, and social support. Our comment does not endorse a specific app. Rather, we observe that health apps frequently operate outside of the clinical ecosystem and are not subject to the same privacy, safety, or quality standards as healthcare-regulated technologies. As a result, patients are exposed to misinformation, privacy & security breaches, and inconsistent navigation support during some of the most vulnerable moments in their care journey. CMS could help us change this.

We believe CMS has a critical opportunity to ensure safer, more trusted alternatives through the following actions:

1. **CMS Billing Structures For Care Navigation:** A vital step forward in recent years has been [Principal Illness Navigation \(PIN\)](#) programs as a way to incentivize care navigation. We urge CMS to consider building upon these programs to enable trained community organizations to provide navigation support where patients struggle to navigate and access care. Doing so creates built-in standards for HIPAA covered entities who refer to these services.
2. **Authorize Community-Based Navigation Entities:** CMS should explore policy pathways that enable **trusted nonprofit and patient-led organizations** to serve as delivery partners for reimbursable digital care navigation services.
3. **Disincentivize conflicts of interest from Payors:** By contrast, we recommend that CMS disincentivize automated services like [NaviHealth](#) that are being used by payors to

charge patients the most amount of money for the least amount of care, or to deny care with AI tools.

4. **Validate Existing Proofs of Concept:** CMS should leverage early successes from public-private partnerships such as [CancerX](#), and other [InnovationX initiatives](#), where community-led organizations are only starting to co-develop **digitally enabled navigation models** that are secure, clinically relevant, and patient-trusted. These models illustrate how software can extend the reach of care coordination—particularly for medically underserved populations—while centering lived experience.
5. **If we had a personal assistant to support our health needs**, we would want:
 - Humans with lived experience are empowered by the best evidence based tools - not merely automated AI chatbots that save money for payors or further dehumanize our experiences in healthcare.
 - Timely, condition-specific guidance to accurate diagnosis, development of care plans, symptom monitoring, and follow-up care.
 - Help to find credible clinical experts, moderated peer support communities, well-vetted research on our conditions, and knowledge shared in terms we understand.
 - A responsive process for feedback and/or reporting problems if things go wrong.
 - A community of experience who incorporate our values and social context into shared decision-making tools *with* patients as partners.
 - Finally, we want AI tools designed in ways that align with the [Patient AI Rights Initiative's](#) guiding principles.

To be effective, the functions of care navigation apps must not solely rely on data monetization business models, or solely for advertising of pharmaceutical ads. The function of care navigation must also be built on CMS reimbursable models that are **patient-aligned, clinically integrated, patient community governed, and scalable infrastructure** that prioritizes safety, fairness, and trust.

VB-1. Incentives for APMs to Adopt Digital Health Navigation Tools

We encourage CMS to support new incentives for digital health adoption that align with the interests of patient outcomes.

1. Reimbursement for Care Navigation Support Tools: CMS should expand the definition of reimbursable services in APMs to explicitly include digital navigation tools that address health literacy, technology access, and culturally responsive communication. Tools like AI-powered chatbots, peer-to-peer messaging platforms, and decision aids for rare diseases must be considered essential components of patient care infrastructure. These tools reduce care fragmentation, particularly for patients with chronic or rare conditions.

2. Inclusion of Patient-Centered Outcomes: Incorporate patient engagement, trust, and confidence metrics into APM performance evaluations. APMs that demonstrate meaningful engagement through digital tools (e.g., increased patient knowledge, goal alignment, or improved self-efficacy) should be eligible for bonus payments. These outcomes should be co-defined with patient communities.

3. Shared Savings Bonuses: Link shared savings payments to the effective use of digitally enabled care navigation solutions. APMs should be rewarded for demonstrable improvements in coordination, reductions in redundant services, and improved patient satisfaction through real-time navigation platforms or digitally-facilitated care plans.

Current Obstacles:

1. Patient Trust and Data Privacy Concerns: Widespread public mistrust—validated in reports like *Tangled In The Web 2024* and the fallout from the 23andMe breach—illustrates why adoption lags. Patients fear misuse of their data, especially by for-profit platforms with opaque business models. Without strong guarantees of data protection and patient governance, uptake will remain limited.

2. Lack of Clear Evaluation Frameworks: Providers lack structured methods for evaluating the safety, fairness, and utility of digital tools. CMS should endorse evaluation frameworks co-developed with patient-led organizations and assign fiduciary responsibilities to independent evaluators. Models like Civic Data Trusts offer a pathway.

3. Infrastructure Limitations: Many providers in rural and underserved communities face insufficient broadband and digital literacy capacity. Federal support must include infrastructure grants and technical assistance programs to support equitable implementation.

VB-2. Integration of Key Themes into Digital Health Certification

1. AI Transparency and Auditability: All AI-driven tools used in Medicare-supported care must be explainable, auditable, and governed through community-inclusive oversight. CMS should encourage the adoption of learning networks like Duke's Health AI Partnership that support local validation and transparency of AI models.

2. Usability Testing with Advocacy Partners: Mandate patient-led usability reviews for all tools used in federally reimbursed care. This ensures accessibility across disability, language, and cultural lines. Advocacy partners should be compensated for this participatory testing, especially for populations with high social vulnerability. Require digital health tools to undergo usability testing through established patient advocacy organizations, to ensure different patient populations to ensure accessibility and effectiveness. One such example for AI, designed and co-authored by patient researchers, shows the difference between clinician vs. patient-led evaluation of LLM's to understand clinical notes and inform decision making. Please check out this great study:

- a. Salmi L, Lewis DM, Clarke JL, Dong Z, Fischmann R, McIntosh EI, Sarabu CR, DesRoches CM. A proof-of-concept study for patient use of open notes with large language models. *JAMIA Open*. 2025 Apr 9;8(2):ooaf021. doi: [10.1093/jamiaopen/ooaf021](https://doi.org/10.1093/jamiaopen/ooaf021). PMID: 40206786; PMCID: PMC11980777.

3. Community-Informed Quality Measurement Systems: CMS should co-design quality metrics with patient and caregiver networks, especially to integrate patient-reported outcomes and community-sourced metrics. Participatory machine learning, as demonstrated in the *PLOS Global Public Health* HIV prevention study (Sendak et al., 2025), provides a model for inclusive metric development.

VB-5 to VB-7: Certification and Compliance Enhancements

To achieve the full promise of value-based care, CMS must modernize its certification and compliance infrastructure to reflect evolving digital capabilities and patient expectations. Traditional ONC certification programs were designed for static EHR systems in fee-for-service models. As healthcare moves toward holistic, team-based, and technology-enabled delivery models, certification requirements must expand to include indicators of digital trust, ethical AI use, and patient-centered interoperability. The following recommendations outline specific gaps in current certification mechanisms and offer actionable pathways to reduce administrative complexity while advancing patient outcomes and innovation.

VB-5. Limitations of Current ONC Certification: The ONC Health IT Certification Program does not adequately address the needs of APMs for social navigation, patient trust-building, and ethics-oriented AI. It must evolve to include non-clinical data use cases and indicators of patient alignment.

VB-6. Missing Capabilities in Health IT Ecosystems:

- **AI Explainability Interfaces:** Interactive tools to demystify algorithmic outputs.
- **Advanced Consent Management:** Granular, context-based consent tracking systems.
- **Outcome Disaggregation Tools:** Disaggregated dashboards for racial, geographic, and gender disparities.
- **Governance Indicators:** Visual transparency into who accesses and acts upon patient data.

VB-7. Streamlining Certification While Preserving Patient Outcomes:

- **Modular Certification Models:** Let APMs mix-and-match certified tools based on unique patient populations.
- **Patient-Centered Certification Tiers:** Offer "Gold Tier" certification for vendors who exceed in ethical design and usability.
- **Regional Innovation Pilots:** Launch limited-scope certifications in states or health systems to test flexibility before scale-up.

VB-8. Supplementing CEHRT Through HHS Policy

1. Extend Event Notification Requirements: Apply real-time ADT notification mandates to all APM participants (not just hospitals). This ensures that all providers involved in care—regardless of size or CEHRT use—can coordinate effectively, reducing readmissions and duplication.

2. Support Community-Based Organizations (CBOs): Provide grants and TA programs to CBOs to adopt digital tools, integrate with health systems, and collect SDOH and patient experience data. CMS should develop a "Digital Readiness Index" to prioritize assistance to high-need communities.

3. Leverage Existing Frameworks: Use NIST AI RMF, Project Evident's learning agenda, and TLC's 7 Requirements for Collective Digital Rights to guide vendors and APMs in implementing ethical, transparent, and fair data practices.

VB-10. CEHRT Flexibility for Advanced APMs

Certification Criteria to Consider:

- **Patient-Specific Consent Data Exchange:** Systems that manage and respect individual patient consent preferences.
- **Federated Data Architecture Support:** Infrastructure that allows for decentralized data management.
- **AI Transparency and Auditing Tools:** Ensure that AI tools used in care are transparent and are subject to regular audits.

Flexibilities for Resource-Constrained Providers:

- **Shared Regional Data Hubs:** Allow smaller APMs to utilize shared resources to meet certification requirements.
- **Funding and Support for Open-Source Tools:** Encourage the development and use of cost-effective, interoperable solutions.
- **Community-Consented Data Exchange:** Enable patient organizations to facilitate data sharing in areas with limited resources.

2. Suggested Resources: Civic Data Trusts as Federated Infrastructure for Patient-Partnered Innovation

Overview

We propose that CMS test and validate patient-governed sandboxes that test two key components: **Federated Patient Infrastructure** and **Civic Data Trusts** through existing and emerging CMMI demonstration models. These approaches empower patient communities—especially those that are struggling to find good knowledge online to navigate care. We hope CMS will prioritize ways to securely steward their data and participate in digital health innovation without being forced into exploitative surveillance platforms.

This concept is aligned with CMS’s strategic refresh of value-based care models, including the **ACO REACH Model** and **AHEAD Model**, which seek to promote better patient outcomes, accountable care delivery, and person-centered transformation.

A. Patient-Governance Sandboxes For Health Tech

1. Federated Patient Infrastructure

Federated Patient Infrastructure refers to a decentralized model for managing health data that prioritizes patient autonomy, ethical governance, and interoperability across care settings. Instead of concentrating data within a single hospital system or proprietary vendor, this ecosystem enables patients to entrust their health data to **community-based intermediaries**, such as patient-led nonprofits or cooperative data stewards, who are accountable to collective interests rather than commercial ones.

These intermediaries facilitate **legally binding governance roles**, allowing patients to determine when, how, and for what purposes their data can be shared—whether for clinical care coordination, research, or AI-supported navigation tools. Critically, all data use in patient governance sandboxes must include **transparency safeguards**, ensuring that algorithms reflect the needs and values of the populations they serve. By avoiding vendor lock-in and enabling shared, values-aligned stewardship, federated infrastructures can resist monopolistic control and foster innovation that is both inclusive and durable.

2. Civic Data Trusts

Civic Data Trusts are legally constituted, community-governed entities designed to manage health-related data on behalf of patient populations in a way that centers public interest, collective accountability, and equity. Unlike traditional data holders, these trusts are fiduciaries for the community, meaning they have a legal and ethical obligation to act in the best interests of the patients whose data they steward.

Rather than solely requiring individual transactional consent, we need a new model that supports collective governance. In the Data Trust legal model, trustees are responsible for setting clear and enforceable rules around how data can be accessed, by whom, and for what purposes—whether for research, quality improvement, or AI deployment in care. Trustees are bound by a fiduciary duty to patients as beneficiaries.

Through collective consent mechanisms, they enable entire patient communities to engage in governance decisions, creating processes for revoking consent, enforcing data access limitations, and redressing misuse. Technically, Civic Data Trusts are designed to integrate with existing Electronic Health Records (EHR) and Health Information Exchange (HIE) infrastructure through open, interoperable standards—ensuring seamless coordination without reinforcing data monopolies. As part of CMMI demonstration models like ACO REACH or AHEAD, these patient-governed sandboxes could serve as authorized data-sharing intermediaries, promoting ethical innovation while strengthening community trust in digital health systems.

B. Possible Implementation Pathways

ACO REACH and the AHEAD Model represent strategic opportunities for piloting Civic Data Trusts because both programs are explicitly designed to address structural inequities in care delivery and incentivize community-based innovation. ACO REACH prioritizes underserved populations and allows for flexible payment models, making it an ideal environment to embed **governance-based care coordination** through partnerships with community-led data intermediaries.

Civic Trusts as a legal framework can facilitate peer navigation and collect community-defined quality metrics, extending the model of accountable care beyond institutional walls. Importantly, ACO REACH's infrastructure and care management payments can be adapted to support the operational costs of Civic Data Trusts, aligning with CMS's emphasis on population health and equity. Meanwhile, the AHEAD Model is focused on **state-level transformation and multi-sector alignment**, particularly around social determinants of health. This makes it a natural fit for testing **federated data infrastructure pilots** in partnership with Medicaid agencies, public health departments, and patient-led organizations. By incorporating Civic Data Trusts into transformation plans, states can not only meet AHEAD's equity benchmarks but also build durable governance models that reflect the lived realities and data rights of their communities.

3. Patient Outcomes and Evaluation Metrics

CMS can strengthen its evaluation strategy by adopting outcome metrics grounded in the Patient AI Rights Initiative's principles of transparency, equity, and collective agency.

1. **For independent duty to patients**, CMS could require reporting of business models or provide standards for data-sharing agreements (such as BAA's) which require higher

standards for certain uses of data. CMS could measure impact of patient negotiations on trust, adoption, and patient outcomes.

2. For **health access improvements**, evaluators should measure not only the increase in digital access among rural or unsupported patient communities, but also the cultural and linguistic relevance of tools, patient-reported ability to find and understand care options, and engagement of historically excluded groups.
3. For **trust and safety**, CMS should track changes in patients' willingness to share data when provided with tools for dynamic consent. CMS could further measure outcomes of transparency metrics for adverse events, and recourse options when harm or misuse occurs.
4. For **cost impact**, metrics should include not only reductions in redundant tests and emergency visits but also improved continuity of care facilitated through ethically governed AI navigation tools and peer network referrals.
5. These indicators can be drawn from participatory evaluation models co-developed with patient organizations and agencies like [AHRQ](#) to ensure they reflect real-world experiences and community-defined value.

4. Citations

Below is a selection of peer-reviewed publications from U.S.-based law and policy journals (2017–2025) that support our public comment. These publications focus on AI policy, **civic data trusts** and **legislating data loyalty** in the context of patient/health data. We hope CMS finds these helpful to inform future policy within this ecosystem.

1. Adler-Milstein, Julia, and Paige Nong. “Early Experiences with Patient Generated Health Data: Health System and Patient Perspectives.” [Journal of the American Medical Informatics Association](#), vol. 26, no. 10, 2019, pp. 952–959.
2. Arora, Chirag. “Digital Health Fiduciaries: Protecting User Privacy When Sharing Health Data.” [Ethics and Information Technology](#), vol. 21, 2019, pp. 181–196.
3. Bartlett, Benjamin. “Towards Accountable, Legitimate and Trustworthy AI in Healthcare: Enhancing AI Ethics with Effective Data Stewardship.” [The New Bioethics](#), vol. 31, no. 1, 2025, pp. 1–25.
4. Bombard, Yvonne, et al. “Engaging Patients to Improve Quality of Care: A Systematic Review.” [Implementation Science](#), vol. 13, 2018, article no. 98.
5. Carman, Kristin L., et al. “Patient and Family Engagement: A Framework for Understanding the Elements and Developing Interventions and Policies.” *Health Affairs*, vol. 32, no. 2, 2013, pp. 223–231.
[pubmed.ncbi.nlm.nih.gov](https://pubmed.ncbi.nlm.nih.gov/pubmed.ncbi.nlm.nih.gov)
6. Centers for Medicare & Medicaid Services. “Request for Information: Health Technology Ecosystem.” *Federal Register*, vol. 90, no. 94, 16 May 2025, pp. 21034–21041. [federalregister.gov](https://www.federalregister.gov)

7. Hartzog, Woodrow, and Neil M. Richards. “Privacy’s Trust Gap: A Review.” *Yale Law Journal*, vol. 126, no. 4, 2017, pp. 1180–1224. [scholarship.law.bu.edu](https://scholarship.law.bu.edu/scholarship.law.bu.edu)
8. Houser, Kimberly A., and John W. Bagby. “The Data Trust Solution to Data Sharing Problems.” *Vanderbilt Journal of Entertainment and Technology Law*, vol. 25, no. 1, 2023, pp. 113–159. [Link](#)
9. National Health Council. ***The National Health Council Patient Engagement Rubric: A Guide to Incorporating the Patient Voice into the Health Ecosystem***. 2019. [Link](#)
10. Obermeyer, Ziad, et al. “Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations.” *Science*, vol. 366, no. 6464, 2019, pp. 447–453. [Link](#)
11. Patient-Centered Outcomes Research Institute (PCORI). ***Foundational Expectations For Partnership***. PCORI, 2024. [Link](#)
12. Porcaro, Keith. “In Trust, Data.” *Minnesota Law Review*, vol. 105, no. 2 (Headnotes), 2021, pp. 332–344. [Link](#)
13. Richards, Neil M., Woodrow Hartzog, and Jordan Francis. “A Concrete Proposal for Data Loyalty.” *Harvard Journal of Law & Technology*, vol. 37, no. 3, 2023, pp. 1335–1387. [Link](#)
14. Skelton-Wilson, Syreeta, Madison Sandoval-Lunn, Xiaodong Zhang, Frances B. Stern, and Jessica Kendall. “Methods and Emerging Strategies to Engage People with Lived Experience: Improving Federal Research, Policy, and Practice.” Office of the Assistant Secretary for Planning and Evaluation, U.S. Department of Health and Human Services, 2021. bettercareplaybook.org