Response to CMS RFI: Health Technology Ecosystem

File Code: CMS-0042-NC

RIN: 0938-AV68

Date: 2025-06-16

Primary Contact Name & Title: **Samir Unni**

Email: **srunni@gmail.com** Phone: **(314) 775-6830**

Centers for Medicare & Medicaid Services
Office of Burden Reduction & Health Informatics
Attn: CMS-0042-NC, Health Technology Ecosystem RFI
7500 Security Boulevard
Baltimore, MD 21244

To Whom It May Concern:

I am pleased to submit the below response, based on my experience working with provider and payer organizations, HHS, and directly with Medicare beneficiaries, particularly dual enrollees, in various capacities over the past decade. I have focused my comments on the practical barriers those patients face when navigating and coordinating their care.

The single most important proposal below is to **re-envision HealthCare.gov as the universal patient front door.** By redesigning and rebranding the existing website so beneficiaries can (1) discover vetted digital-health tools, (2) authenticate once with a trusted credential such as Login.gov, and (3) grant downstream apps seamless access to payer and provider data, CMS can address the awareness and trust hurdles that currently frustrate patients and caregivers, when it comes to utilizing digital health products. All other patient- or caregiver-facing improvements—price-shopping, appointment scheduling, intake-form automation, and real-time care navigation—depend on that foundational step.

Thank you for the opportunity to comment and for your continued efforts to modernize the health-technology ecosystem for America's seniors and their families.

Sincerely,

Samir Unni

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?

- a. What are the top things you would like to be able to do for your or your loved ones' health that can be enabled by digital health products?

> ***The single most important problem that a digital health product could personally solve for me would be to make it easier to manage the healthcare received by my elderly loved ones, particularly my parents, who are both on Medicare.***
>
> ***By providing the infrastructure to enable care navigation technology innovators to tackle this problem, CMS can improve the lives and health outcomes of Medicare beneficiaries, while also reducing its own expenses on care navigation. Empowering the adult children of Medicare beneficiaries, to more seamlessly shoulder responsibilities that many of them already have, is a critical complement to reimbursing third-party care navigators.***

PC-2. Do you have easy access to your own and all your loved ones' health information in one location (for example, in a single patient portal or another software system)?

No, easy access to health information in one location is currently not possible, due to:

- ***Limited support, in practice, for the Individual Access Services (IAS) Exchange Purpose (XP), in TEFCA, despite IAS being a required XP.***
  - ***This is largely due to unresolved concerns, on the parts of the QHINs, about HIPAA liability resulting from incorrect patient matches.***
  - ***As a result, users are forced to authenticate with each (Sub)Participant from which records are available***
- ***Limited exchange of health information between payers and providers, preventing me from obtaining that information from just one payer or provider***
- ***Limited support for obtaining machine-readable copies of health information from payers or providers***
  - ***Certified EHR Technology has not been adopted by many providers who do not participate in Medicare, such as on-site clinics at employers.***
  - ***Where Certified EHR Technology has been adopted, production implementations have not been tested for performance. It is not***

uncommon to encounter significant downtime, or for crucial data elements to be left blank in responses to FHIR API calls.

- ***The payer Patient Access API has not been adopted by many health plans who are not regulated by it, such as commercial health plans, or ACA plans on state-based exchanges.***
- ***Even where the Patient Access API has been adopted by CMS-regulated health plans, it often returns incomplete data in practice. Once again, a failure to test production implementations has left major gaps in real world API performance.***

- ***The imposition of periodic reauthentication requirements, by payer and provider APIs. This means that reauthentication is often required at the very moment that a beneficiary tries to use a digital health product or experience, incentivizing them to instead rely on traditional means of accessing healthcare services.***

- a. If so, what are some examples of benefits it has provided?

There are currently limited benefits to having the health information I do currently have access to. Not only is the available information largely clinical in nature, but it's also disconnected from the largely administrative workflows that I (and my loved ones) personally engage in, such as scheduling appointments or filling out forms.

- b. If not, in what contexts or for what workflows would it be most valuable to use one portal or system to access all such health information?

In administrative workflows. For instance, not having to manually supply my demographic and coverage information at the beginning of every visit, because those forms were automatically filled out by an AI agent that has access to my health information, would be very valuable.

PC-4. What features are missing from apps you use or that you are aware of today?

- b. What set of workflows do you believe CMS is uniquely positioned to offer?

CMS is uniquely positioned to offer the crucial digital health product discovery workflow (i.e., the front door) for Medicare beneficiaries, by repurposing and rebranding HealthCare.gov. See the answer to PC-6 for more details.

PC-5. What can CMS and its partners do to encourage patient and caregiver interest in these digital health products?

- a. What role, if any, should CMS have in reviewing or approving digital health products on the basis of their efficacy, quality or impact or both on health outcomes (not approving in the sense of a coverage determination)? What criteria should be used if there is a review process? What technology solutions, policy changes, or program design changes can increase patient and caregiver adoption of digital health products (for example, enhancements to data access, reimbursement adjustments, or new beneficiary communications)?

  CMS should review and approve digital health products insofar as it promotes them—which it should do by repurposing, and rebranding, HealthCare.gov into a universal front door, for access to healthcare. Doing so is by far the most important role that CMS can play in accelerating the uptake of digital health products by Medicare beneficiaries.

  Note that primary responsibility for reviewing and approving digital health products on the basis of their efficacy, quality, or impact on health outcomes, should lie with FDA, not CMS.

- b. What changes would enable timely access to high quality CMS and provider generated data on patients?

  As described in the answer to PC-9(b), adding support, to the Blue Button 2.0 API, for retrieving Part C claims, for Medicare beneficiaries on MA plans, is the most important step CMS can take to enable timely access to high quality CMS generated data on patients.

  Accelerating participation by providers in TEFCA IAS, by making the changes described in PC-10(b), is the most important step CMS can take to enable timely access to high quality provider generated data on patients.

PC-6. What features are most important to make digital health products accessible and easy to use for Medicare beneficiaries and caregivers, particularly those with limited prior experience using digital tools and services?

The single biggest barrier to accessibility and ease of use of digital health products, by Medicare beneficiaries and caregivers, is a lack of awareness, as to which products and services are available.

CMS can address this shortcoming by repurposing, and rebranding, HealthCare.gov as the universal front door for access to healthcare, rather than being just for the ACA Marketplace.

This could include a vetted "app marketplace."

PC-7. If CMS were to collect real-world data on digital health products' impact on health outcomes and related costs once they are released into the market, what would be the best means of doing so?

If CMS were to introduce, and incentivize the use of, a single, federated identity provider (such as Login.gov) for all digital health experiences for Medicare beneficiaries, it would have direct access to digital health product authentication metrics for Medicare beneficiaries. It can then cross-reference those metrics with outcomes, based on the beneficiary claims data that CMS already collects.

PC-8. In your experience, what health data is readily available and valuable to patients or their caregivers or both?

- a. What data is valuable, but hard for patients and caregivers, or app developers and other technical vendors, to access for appropriate and valuable use (for example, claims data, clinical data, encounter notes, operative reports, appointment schedules, prices)?

Prescription drug price data, particularly the historical net price and cost-sharing liability, for every Part D and MAPD plan, should be publicly available. This would enable both CMS and Medicare beneficiaries to save billions of dollars a year on prescription drug spend. Congress granted CMS authority to require that information to be published, by the plans, in CAA 2021, and CMS issued an associated regulation (the Health Plan Price Transparency Final Rule), but has chosen not to enforce it for several years.

PC-9. Given that the Blue Button 2.0 API only includes basic patient demographic, Medicare coverage, and claims data (Part A, B, D), what additional CMS data sources do developers view as most valuable for inclusion in the API to enable more useful digital products for patients and caretakers?

- a. What difficulties are there in accessing or utilizing these data sources today?

  Yes. The Blue Button 2.0 API currently only returns Part D claims for Medicare beneficiaries on MAPD plans.

- b. What suggestions do you have to improve the Blue Button 2.0 API experience?

  The Blue Button 2.0 API should be updated to return Part C claims for Medicare beneficiaries on MA plans (once they have been submitted to CMS by those MA plans). While these claims are often available directly from MA plans via the Patient Access API, adding support in Blue Button 2.0 reduces the burden on Medicare beneficiaries attempting to retrieve those claims, as they would not need to authenticate into individual MA plan portals.

- c. Is there non-CMS data that should be included in the API?

  Yes.

PC-10. How is the Trusted Exchange Framework and Common Agreement TM (TEFCA TM) currently helping to advance patient access to health information in the real world?

- a. Please provide specific examples.

  TEFCA's impact on advancing patient access to health information, through the IAS XP, is unfortunately currently minimal.

- b. What changes would you suggest?

  A major shortcoming of TEFCA IAS is that Record Locator Services are currently operated by individual QHINs, and thus present heterogeneous user experiences to patients, depending on which QHIN their providers happened to be participating in TEFCA through. For instance, Epic, in its capacity as a QHIN, currently requires that each patient individually authenticate with each Participant (i.e., Epic customer) at which they have records. This is

required due to the liability that would be incurred, by Epic and/or their customers, in the event of an improper disclosure of PHI, resulting from an incorrect match of the end user to a given patient record at an Epic customer that is a TEFCA Participant.

CMS can rectify this shortcoming in two phases:
1. In the short run, by partnering with HHS OCR to exercise enforcement discretion, with respect to the HIPAA Privacy Rule, for improper disclosures of PHI, by TEFCA QHINs and (Sub)Participants, for the IAS XP, due to incorrect patient matches. For instance, a safe harbor could be created for any such improper disclosures that occur via a QHIN using an ASTP-approved patient matching algorithm. The ONC Patient Matching Challenge, from 2017, has plenty of prior art to draw on, for which algorithms should be approved for a safe harbor.
2. In the long run, by having the RCE operate a centralized RLS that supports CMS/ASTP-approved digital identity credentials.

- c. What use cases could have a significant impact if implemented through TEFCA?

Care navigation applications would become much easier to use if implemented through TEFCA, as they would be able to seamlessly take into account the user's medical history, as well as where they had received care in the past.

- g. Are there adequate alternatives outside of TEFCA for achieving widespread patient access to their health information?

No, there are not.

PC-11. How are health information exchanges (HIEs) currently helping to advance patient access to health information in the real world?

- a. How valuable, available, and accurate do you find the data they share to be?

While HIEs play an important role in the health tech ecosystem and care delivery landscape today, they are highly variable in terms of the accuracy and freshness of the data they deliver.

- b. What changes would you suggest?

Over time, CMS and ASTP should consolidate all existing use cases that rely on HIEs to TEFCA. This will reduce provider IT overhead

associated with accessing and utilizing overlapping interoperability networks.

PC-13. How can CMS encourage patients and caregivers to submit information blocking complaints to ASTP/ONC's Information Blocking Portal? What would be the impact? Would increasing reporting of complaints advance or negatively impact data exchange?

The single biggest step that CMS/ASTP can take to encourage patients and caregivers to submit information blocking complaints to the Information Blocking Portal is to rapidly and publicly action submitted information blocking complaints, so that the public sees evidence that submission of complaints produces real results.

PC-14. Regarding digital identity credentials (for example, CLEAR, Login.gov, ID.me, other NIST 800-63-3 IAL2/AAL2 credentialing service providers (CSP)):

- a. What are the challenges today in getting patients/caregivers to sign up and use digital identity credentials?

The single biggest challenge, in getting patients/caregivers to sign up and use digital identity credentials from NIST 800-63-3 IAL2/AAL CSPs, is that they are not useful today. The vast majority of digital health product experiences do not offer authentication options that utilize credentials from those CSPs. Most importantly, that includes CMS-regulated plans' member portals and Certified EHRs' patient portals.

For instance, the vast majority of Certified EHR's patient portals, and CMS-regulated plan's member portals, do not support user authentication with credentials from one of those CSPs. Even CMS's own beneficiary-facing website, Medicare.gov, does not have support for such an option.

- b. What could be the benefits to patients/caregivers if digital identity credentials were more widely used?

More widespread use of digital identity credentials, from NIST 800-63-3 IAL2/AAL CSPs, is the single biggest step that CMS could take to empower Medicare beneficiaries and their caregivers to access and utilize digital health products and experiences.

Without identity verification and authentication experiences that

are user friendly while also meeting enterprise security requirements, any downstream efforts to design and build digital health products will not reach the vast majority of Medicare beneficiaries. Today, they struggle with the status quo of password-first, multifactor authentication workflows.

- c. What are the potential downsides?

    1. ***If not implemented with the user (Medicare beneficiary) experience kept top of mind, the identity verification and/or authentication experiences will prove far too cumbersome for Medicare beneficiaries to complete.***

       For instance, the current IAL2 identity verification experience often involves the use of a mobile device's camera to take pictures of oneself and/or one's photo ID. Requiring users to complete such a step will inevitably result in the vast majority of Medicare beneficiaries opting out.

    2. ***If CMS-regulated plans and Medicare providers do not offer digital experiences that support digital identity credentials, Medicare beneficiaries will be confused by heterogeneous identity verification and authentication experiences.***

- d. How would encouraging the use of CSPs improve access to health information?

    The use of CSPs would allow Medicare beneficiaries to utilize digital identity credentials that they already have and use for other purposes. For instance, Login.gov can also be used to authenticate with SSA, allowing Medicare beneficiaries to develop familiarity with how to use Login.gov prior to when they need to access care.

- e. What role should CMS/payers, providers, and app developers have in driving adoption?

    CMS, other payers, providers, and app developers can all help drive adoption of digital identity credentials by making them the default means of authentication in their digital health products and experiences.

    In particular, CMS can use its regulatory authority to ensure digital identity credential support in authentication flows provided to

patients by CMS-regulated plans and providers using Certified EHR Technology. See the answer to PC-14(f) for more details.

- f. How can CMS encourage patients to get digital identity credentials?

  First, CMS should immediately use its regulatory authority to mandate the use of a single identity provider by CMS-regulated health plans, in their member-facing digital health experiences, and in Certified EHR Technology, for patient portals. Ideally, that mandated identity provider is Login.gov, which is already being widely adopted across a variety of government services. This step should be taken by CMS right away, as it will take time for CMS-regulated plans and Certified EHR Technology developers to implement support for Login.gov.

  Next, CMS should partner with the GSA's Technology Transformation Services (TTS) team to implement support for passwordless-authentication in Login.gov, at the IAL2 assurance level. Specifically, Login.gov should support authentication with ID cards that have both NFC chips and fingerprint readers. Between the ID card itself (something the user possesses), the fingerprint reader (something the user is), and its NFC functionality, users should be able to obtain digital identity credentials on modern consumer technology devices without having to remember and enter a password, or other secret.

  Finally, CMS should offer Medicare beneficiaries updated Medicare Cards, with built-in NFC and a fingerprint reader, that beneficiaries can opt into. CMS should then pilot the use of these cards, with a volunteer cohort of early adopter Medicare beneficiaries. In that pilot, CMS should aim to measure a demonstrable increase in utilization of digital health experiences by beneficiaries. Upon successful pilot completion, CMS should partner with the Medicare broker community to distribute updated identity cards, as well as complete the initial identity proofing process.

PR-4. What changes or improvements to standards or policies might be needed for patients' third-party digital products to have access to administrative workflows, such as auto-populating intake forms, viewing provider information and schedules, and making and modifying an appointment?

Fundamentally, in order to unlock such administrative workflows in third-party digital products, CMS and ASTP must refocus digital

health interoperability initiatives away from the gradual addition, via new regulations, of ever more clinical data elements to the FHIR APIs required of Certified EHRs, and towards a workflow-first approach that prioritizes improving the administrative experience for patients and their caregivers.

The most effective way to accomplish that is to measure, and hold provider organizations / Certified EHR technology developers accountable to, outcomes, rather mandating the addition of capabilities. For instance, CMS should require providers to measure, and improve on, year over year, metrics such as:
- The percentage of intake forms that can be populated in third party digital products
- The percentage of providers for whom open scheduling is supported
- The percentage of appointments that are scheduled, and rescheduled, via open scheduling

---

PR-9. How might CMS encourage providers to accept digital identity credentials (for example, CLEAR, ID.me, Login.gov) from patients and their partners instead of proprietary logins that need to be tracked for each provider relationship?

- a. What would providers need help with to accelerate the transition to a single set of trusted digital identity credentials for the patient to keep track of, instead of one for each provider?

The vast majority of patient-facing digital health experiences available from providers are built on technology from Certified EHR Technology vendors. CMS can encourage the acceptance of digital identity credentials by making support for them, in patient-facing Certified EHR Technology, a Condition of Certification.

- b. How might CMS balance patient privacy with convenience and access to digital health products and services that may lead to significant improvements in health?

As described in the answer to PC-14(f), CMS should utilize passwordless authentication by leveraging smart ID cards that support NFC and have fingerprint readers, such that IAL2 remote identity proofing is possible in a workflow that is truly usable for Medicare beneficiaries.

TD-1. What short term (in the next 2 years) and longer-term steps can CMS take to stimulate developer interest in building digital health products for Medicare beneficiaries and caregivers?

In order to drive real change on a 2-year timescale, CMS needs to address three major current obstacles to the development of digital health products:

1. <u>Awareness</u>: Medicare beneficiaries/caregivers are generally not aware of these products, and which are most relevant to them. Driving that awareness is an expensive proposition for digital health product developers
2. <u>User experience</u>: Medicare beneficiaries cannot rapidly authenticate into those digital health products' experiences and grant them access to one's own medical history.
3. <u>Business model</u>: in order to sustain their own existence, digital health product developers have to identify a third party (e.g., a health plan) with a vested interest in improving outcomes for the Medicare beneficiaries who are their users, and execute an enterprise sale to that third party.

CMS can short circuit this convoluted process, in order to see real results within 2 years, by:
1. Repurposing and branding HealthCare.gov as the universal healthcare front door for patients, particularly Medicare beneficiaries. See the answer to PC-6 for more details.
2. Implementing an identity verification and authentication experience that is usable for all patients, particularly Medicare beneficiaries with limited digital literacy. See the answer to PC-14 for more details.
3. Partnering with ASTP and the TEFCA RCE to implement a single RLS, so that patients only have to authenticate once. Currently, RLS's are being implemented at the QHIN level, effectively forcing patients to repeatedly authenticate. See the answer to PC-10(b) for more details.
4. Contracting with digital health product developers, through Innovation Models, to directly pay them for interventions that meaningfully improve health outcomes for Medicare beneficiaries.

TD-3. Regarding digital identity implementation:

- a. What are the challenges and benefits?

  The primary challenge is that digital identity credentialing workflows are often far too complex for the majority of Medicare beneficiaries to utilize. In order to ensure they do not end up unused by the target user group, CMS must pilot, and iterate on, those workflows, with focus groups of real Medicare beneficiaries.

- b. How would requiring digital identity credentials (for example, CLEAR, Login.gov, ID.me, other NIST 800-63-3 IAL2/AAL2 CSPs) impact cybersecurity and data exchange?

  Using digital identity credentials, particularly from Login.gov, can provide the Service Provider with additional demographic information (ex: SSN) that can be used to match a user to health records that they already have, thereby reducing the likelihood of improper health data disclosure.

TD-7. To what degree has USCDI improved interoperability and exchange and what are its limitations?

- a. Does it contain the full extent of data elements you need?

  No, it does not.

- b. If not, is it because of limitations in the definition of the USCDI format or the way it is utilized?

  It is because of both.

- c. If so, would adding more data elements to USCDI add value or create scoping challenges? How could such challenges be addressed?

  USCDI has mistakenly focused on clinical data interoperability, to the detriment of improving the administrative workflow experience for users. The most important missing data elements in USCDI are regarding scheduling, while the most important missing workflows are those that all of us regularly experience when interacting with the medical system: completing intake forms, refilling medications, and communicating with provider staff. None of these activities should be gatekept to workflows in proprietary mobile/web apps from EHR vendors.

- d. Given improvements in language models, would you prefer a non-proprietary but less structured format that might improve data coverage even if it requires more processing by the receiver?

  Yes, the focus on exquisitely structuring all data transmitted via interoperability APIs has dramatically held back the pace at which new data elements are added to those APIs.

  There are two distinct groups of use cases to be addressed:
  1. Administrative workflows, which require a structured read AND write framework, for third-party applications to interact with Certified EHRs.
  2. Health data retrieval workflows, which can consist of a semi-structured dump of all of my health data, which a language model can then parse for me. EHI Export has created a solid foundation, upon which to build, for this group of use cases.

TD-11. As of January 1, 2024, many health IT developers with products certified through the ONC Health IT Certification Program are required to include the capability to perform an electronic health information export or "EHI export" for a single patient as well as for patient populations (45 CFR 170.315(b)(10)). Such health IT developers are also required to publicly describe the format of the EHI export. Notably, how EHI export was accomplished was left entirely to the health IT developer. Now that this capability has been in production for over a year, CMS and ASTP/ONC seek input on the following:

- a. Should this capability be revised to specify standardized API requirements for EHI export?

  Yes.

- b. Are there specific workflow aspects that could be improved?

  Yes, there should also be a requirement that the standardized API can be accessed, without any additional authentication steps, from within patient portals.

- c. Should CMS consider policy changes to support this capability's use?

  Yes, it should implement new Conditions of Certification for EHI Export, including standardized API requirements and patient portal support.

TD-19. Regarding price transparency implementation:

- a. What are current shortcomings in content, format, delivery, and timeliness?

The primary shortcoming of the current implementation of price transparency is that there is no enforcement of data quality standards, resulting in highly variant and spotty data, with significant backsliding since the initial deadline. CMS can rectify these shortcomings in either of these ways:
1. Switch to a portal-based approach, whereby impacted health plans and hospitals upload their transparency data files to a CMS system, which confirms and approves the upload, as meeting a data quality bar. Consumers of the data could then obtain it directly from CMS.
2. Develop and establish a system for actively monitoring the contents of publicly posted price transparency files and penalize impacted health plans and hospitals who are found not to be in compliance.

Second, price transparency regulations currently do not extend to Part D rates, as CMS has delayed enforcement for years.

- b. Which workflows would benefit most from functional price transparency?

The single most important workflow that would benefit from functional price transparency is generic drug fills. There is often significant variance in the prices of generic drugs between pharmacies, and consumers will be incentivized to use this workflow, because of the potential for out-of-pocket savings.
