Response to Request for Information on Health Data Interoperability and Digital Health Technology

RE: Response to Request for Information (RFI) – CMS-0042-NC

Submitted By:
Unite
taner@uniteyourhealth.com

To:
Centers for Medicare & Medicaid Services (CMS)
Department of Health and Human Services
Attention: CMS-0042-NC
P.O. Box 8013
Baltimore, MD 21244-8013
Assistant Secretary for Technology Policy/Office of the National Coordinator for Health Information Technology (ASTP/ONC)

Unite respectfully submits this response to the Request for Information (RFI) regarding the digital health product market, data interoperability, and health technology infrastructure, as published in the Federal Register.

We commend the Centers for Medicare & Medicaid Services (CMS) and the Assistant Secretary for Technology Policy/Office of the National Coordinator for Health Information Technology (ASTP/ONC) for their continued leadership and commitment to advancing a patient-centered digital health ecosystem. The policy framework established by the 21st Century Cures Act has laid a critical foundation for innovation.

Unite is the data & AI platform for healthcare, integrating with existing CMS systems. Unite is deployed with leading healthcare providers, research organizations, and pharma companies.

As a technology organization at the forefront of developing and deploying patient-facing digital health applications, Unite has direct, real-world experience navigating the complexities of the current interoperability landscape. Our engineering and product teams engage daily with the technical, operational, and policy realities of connecting to

provider and payer APIs across the country. This response is grounded in that practical experience over 8 years.

We share your assessment that while the building blocks for a patient-centric digital health ecosystem are in place, the experience for most stakeholders is "neither seamless nor simple". To bridge this gap, we believe a series of targeted, technically-grounded, and mandatory policy interventions are necessary.

The following comments provide specific, actionable recommendations designed to dismantle systemic barriers, stimulate a dynamic and competitive digital health marketplace, and at last deliver on the promise of straightforward, secure, and meaningful access to health information for both patients and caregivers.

We thank you for the opportunity to provide this feedback and welcome further dialogue on these critical issues.

Executive Summary

The vision of a connected, patient-centric learning health system, as enabled by the 21st Century Cures Act, remains partially realized. While foundational policies have established a framework for interoperability, systemic technical and procedural barriers erected by incumbent actors continue to stifle innovation, frustrate patients, and prevent the emergence of a truly seamless digital health experience. The current ecosystem is characterized by information asymmetry, inefficient data access paradigms, and inconsistent implementation of standards, which collectively undermine the goals set forth by CMS and ASTP/ONC.

Unite, a healthcare technology organization with extensive, hands-on experience building and deploying patient-facing applications, has identified a set of critical, interdependent interventions that are required to overcome these challenges. Our recommendations are not theoretical. They are derived from the daily realities of integrating with certified health IT implementations and designed to be both technically sound and immediately actionable.

To accelerate progress and deliver on the promise of patient-centered digital health, Unite urges CMS and ASTP/ONC to adopt the following interconnected recommendations:

- **Mandate a National Provider-to-FHIR Endpoint Directory.** The single greatest practical impediment to patient data access is the inability to reliably locate the correct Fast Healthcare Interoperability Resources (FHIR®) Application Programming Interface (API) endpoint. CMS must mandate the creation of a centralized, publicly accessible directory, populated and maintained by Certified Health IT developers in collaboration with their customers and hosted by CMS in partnership with the National Plan and Provider Enumeration System (NPPES). This is the foundational infrastructure upon which all other API-based policies depend.
- **Prohibit Anti-Competitive Authorization Practices.** To protect patient choice and foster trust, CMS and ONC must explicitly prohibit the use of "scare screens" and other manipulative tactics in the SMART® on FHIR authorization workflow. These practices, employed by dominant market actors, represent a form of information blocking and must be met with vigorous enforcement.
- **Modernize Data Exchange for Patient Apps with Bulk FHIR and Subscriptions.** The current model of polling for data one resource at a time is architecturally unsustainable and may soon create an immense burden on both developers and provider systems. CMS must mandate support for patient-authorized *HL7® FHIR Bulk Data Access* for comprehensive data retrieval and *HL7 FHIR Subscriptions* for real-time event notifications, aligning the ecosystem with established, modern, scalable standards.
- **Establish Ecosystem-Wide Accountability and Support around Reported Bugs in APIs.** A mature digital infrastructure requires professional-grade support. CMS could enable accelerated innovation across the ecosystem with a simple pair of actions: mandating that all certified API endpoints have a monitored technical contact and establishing a centralized, public bug-reporting platform to ensure transparency and timely resolution of technical issues.
- **Align Financial Incentives and Enforcement Actions.** Policy must be paired with powerful incentives and disincentives. We recommend tying a portion of Medicare Advantage payments directly to full and demonstrable API compliance and clarifying that the technical and procedural failures detailed in this response constitute Information Blocking practices subject to established penalties.

These recommendations form a cohesive and comprehensive roadmap. Implemented together, they will dismantle the most significant barriers to interoperability, foster a vibrant and competitive market for digital health innovation, and finally provide patients and caregivers with the simple, secure, and meaningful access to health information they were promised.

Section I: Introduction and Company Background

Unite is a health analytics and personalized engagement platform that uses electronic health records (EHR), a direct relationship with patients, and world class analytics systems to understand where each patient is in their journey and unlock optimal care pathways. Unite's platform connects to over 19,000 health systems in the U.S., giving it the unique ability to access and leverage real-time data flows for over 95% of patients across the country upon joining Unite's platform.

Our mission is to empower individuals with innovative digital tools that simplify the healthcare journey, prevent chronic disease, facilitate participation in research, and enable better health outcomes. We are dedicated to realizing the vision of a connected, patient-centered digital ecosystem as envisioned by the 21st Century Cures Act and subsequent federal rulemaking.

Our perspective and recommendations are not based on theoretical analysis. They are forged from years of direct, hands-on experience. Unite's platform has been in use by real patients pulling real data from real healthcare provider systems across the United States since 2019.

The Unite team comprises engineers (with deep expertise in cybersecurity, big data, software infrastructure, & AI), clinicians, product developers, and healthcare industry leaders who have spent years building, deploying, and maintaining patient-facing applications that connect to thousands of disparate Electronic Health Record (EHR) systems and payer APIs across the United States.

We have engaged directly with the full spectrum of FHIR implementations—from best-in-class systems to those that barely meet certification requirements. We have navigated the fragmented landscape of endpoint discovery, contended with non-standard authorization workflows, and engineered complex solutions to overcome the inefficiencies of current data access paradigms.

This deep, practical expertise provides us with a unique vantage point on the state of interoperability. We understand the specific technical and operational friction points that hinder progress and prevent the market for digital health products from reaching its full potential. The feedback provided in this document is therefore grounded in the "implementation realities" of the current ecosystem. It is offered in a spirit of

constructive partnership, with the goal of providing CMS and ASTP/ONC with the specific, technically-grounded insights necessary to craft effective, durable, and transformative policy.

Section II: Recommendations for a Further Modernized Interoperability Framework

To achieve the seamless, simple, and patient-centric experience described in the RFI, CMS and ASTP/ONC must address a series of fundamental architectural and operational deficiencies in the current health IT ecosystem. The following sections detail our highest-priority recommendations pertaining to the RFI questions, organized thematically to present a cohesive strategy for systemic improvement. Each recommendation is designed to be a specific, enforceable, and technically sound mandate that directly aligns with the stated goals of the agency.

Subsection 2.1: Establishing a National Provider-to-FHIR Endpoint Directory: The Foundational Layer for Discovery

RFI Questions Addressed: TD-5, PR-4, TD-2, TD-15, PR-10, VB-15

Issue Identification: The single most significant practical barrier to patient-directed data exchange today is the lack of a reliable, authoritative, and publicly accessible directory of provider FHIR API endpoints; metadata describing which healthcare professionals, provider organizations, and organization clinic and practice locations provide data through each endpoint; documentation of limitations in data coverage by that endpoint; and documentation of deviations from the reported versions of the standardized implementation specs. Third-party application developers, the very innovators CMS seeks to encourage, have no standardized method to discover the correct electronic address for a patient's data. This is not a minor inconvenience; it is a fundamental infrastructure failure that renders the promise of API access moot for hundreds of millions of patients.

Real-World Impact Analysis: The absence of a central directory creates an untenable situation where every application developer must independently attempt to build and maintain a proprietary map of the nation's FHIR endpoints. This process is

manual, brittle, and perpetually out of date. It leads to high rates of connection failures, which manifest to the end-user—the patient or caregiver—as an error message stating their provider cannot be found. This experience erodes user trust, leads to application abandonment, and directly contradicts the goal of a "seamless" patient journey.[1] This information asymmetry creates a market failure, where only the incumbent EHR vendors possess a comprehensive map of their own endpoint landscape, stifling the competition and innovation CMS wishes to foster.

Proposed Solution: To remedy this foundational deficit, CMS, in partnership with NPPES, must mandate the creation of and subsequently host a centralized, publicly accessible **National Provider-to-FHIR Endpoint Directory**. This directory must be treated as a core component of the nation's health IT infrastructure.

1. **Mandatory Registration by Certified Health IT Developers:** The legal and technical obligation to populate and continuously maintain accurate endpoint information *must* be placed upon the developers of Certified Health IT. These vendors are the sole source of truth for their systems' configurations, geographic coverage, supported standards, and operational status. This should be a mandatory Condition of Certification under the ONC Health IT Certification Program.[1]
2. **Public, Machine-Readable Access:** The directory must be made available to the public at no cost. It must be fully machine-readable via a RESTful API and also offer secure bulk data export functionality to support a wide range of use cases for developers, researchers, and other stakeholders.
3. **Comprehensive Data Elements:** The directory must be sufficiently detailed to enable robust, unambiguous endpoint resolution. At a minimum, it must include the data elements specified in Table 1.

Justification and Alignment with CMS Goals: This proposal directly answers RFI questions TD-5 ("How could a nationwide provider directory of FHIR endpoints improve access?") and VB-15 ("What key data elements would be necessary...?"). It provides the foundational infrastructure necessary to make all other API-based policies functional. By dramatically reducing friction for developers and enabling reliable, patient-directed queries, it is the single most important step CMS can take to "reduce barriers to data access" and accelerate progress towards a "patient-centric learning health system".[1] Creating this directory transforms endpoint discovery from a proprietary, competitive hurdle into a public utility, analogous to the Domain Name System (DNS) for the internet, thereby correcting a critical market failure and fostering a more open and competitive ecosystem.

Table 1: Required Data Elements for a National Provider-to-FHIR Endpoint Directory

Data Element	Resource or Source	Description	Ecosystem Value
Provider Organization Info			
Organization Name & Aliases	$Organization.name, $Organization.alias	The official legal name and all commonly used names (d.b.a., patient-facing brands) for the provider organization.	Enables patient-friendly search and disambiguation, as patients often know their hospital by a brand name, not its legal entity name.[1]
Locations & Addresses	$Location.name, $Location.address	A complete list of all physical locations (hospitals, clinics) associated with the organization and its FHIR endpoint(s).	Allows patients to find their records based on where they received care, a primary search vector for users.[1]
Website URL	Custom Extension or Documentation	The primary public-facing website for the provider organization.	Provides a human-readable fallback for users to find more information.
Clinician NPIs	$Practitioner.identifier (NPI)	An up-to-date list of National Provider Identifiers for all clinicians who practice at the organization's locations.	Enables users to find their records by searching for their specific doctor, a critical and common workflow.[1]
Technical Endpoint Metadata			
FHIR Base URL	$Endpoint.address	The base URL for the production FHIR API endpoint.	The fundamental technical address required for any API interaction.
Supported Standards Versions	$CapabilityStatement (fully populated)	The specific versions of key standards supported, including FHIR (e.g., 4.0.1), SMART App Launch (e.g., 2.2.0), and US Core IG (e.g., 6.1.0).	Prevents version mismatch errors and allows apps to tailor requests to what the server can support, reducing failures.
Deviations & Extensions	Vendor Documentation	Publicly accessible documentation detailing	Critical for developers to handle vendor-specific

Data Element	Resource or Source	Description	Ecosystem Value
		any deviations from the supported US Core IG, including all custom extensions, profiles, or use of contained resources.	nuances, which are a major source of integration complexity and failure.
Data Mapping Logic	Vendor Documentation	Detailed documentation of the source data and logic used to populate each FHIR resource field.	Provides essential transparency for developers to understand the provenance and meaning of the data they receive.
Patient Experience & Testing			
Patient Portal Login URL	Custom Extension or Documentation	The direct URL to the login page of the patient portal whose data serves the FHIR endpoint.	Simplifies the user experience by allowing apps to direct users to the correct login page during the authorization flow.
Provider-specific Public Test Sandbox	Vendor Documentation	A link to a publicly accessible test sandbox environment for the endpoint, with supporting documentation and test data.	Essential for developers to test their applications without needing a production account, dramatically lowering the barrier to entry.
Bulk Data for Directory Building			
Bulk Org/Practitioner/Location Export	Bulk FHIR Export	Mandate that certified systems provide a bulk export of their full $Practitioner, $Location, and $Organization resources.	Enables third parties to build and enhance their own provider directories and patient-matching tools, fostering a richer ecosystem.

Subsection 2.2: Ensuring Patient Trust and Autonomy in Application Authorization

RFI Questions Addressed: TD-18, TD-10, PR-12, PC-13

Issue Identification: The integrity of the patient authorization process, a cornerstone of the 21st Century Cures Act, is being actively undermined by certain dominant Certified Health IT developers. These vendors have implemented non-standard application registration processes that include subjective questionnaires about an application's business model or data use practices. Based on the responses, they then inject intimidating and misleading warning messages—so-called "scare screens"—into the standard SMART on FHIR authorization workflow patients undergo to connect their records to an app.

Real-World Impact Analysis: Third party apps, by their very nature, already have a significant vested interest in ensuring their practices align with the expectations of patients and caregivers, since the app developer's business model would be entirely at risk if patients were to stop trusting the app and its developers. As such, we fear that this practice by developers of certified health IT of injecting frightening warning messages during the authorization process may not be a good-faith effort to protect patients; it is a highly effective business strategy that uses Fear, Uncertainty, and Doubt (FUD) to manipulate patient choice. By displaying messages with large red "X"s and cautionary language, these vendors deter patients from using legitimate, innovative third-party applications that may compete with the vendor's own offerings or business partners. This erodes patient trust in the very digital health ecosystem CMS is trying to build, directly subverts patient autonomy, and functions as a powerful anti-competitive tool. It is a textbook example of a practice that interferes with the access, exchange, and use of electronic health information by patients and caregivers.

Proposed Solution: CMS and ONC must take immediate and decisive action to preserve the neutrality and integrity of the patient authorization process.

1. **Explicit Prohibition:** Issue guidance that explicitly prohibits the use of "scare screens" or similar tactics in the SMART on FHIR authorization experience, or alteration of the standard neutral process—including its visual presentation, text, and workflow—based on proprietary, non-transparent, or subjective vendor criteria. The patient-facing authorization screen must be neutral, factual, and consistent across all certified systems.
2. **Standardize App Registration:** Mandate a standardized, streamlined, and purely technical app registration process for all Certified Health IT. Onerous, subjective questionnaires designed to screen for business preferences, rather than technical conformance, must be eliminated.
3. **Vigorous Enforcement via Information Blocking Rules:** Define the use of "scare screens" and other manipulative authorization tactics as a *per se* violation of the Information Blocking regulations (45 CFR Part 171). This provides a clear and

powerful enforcement pathway with significant financial disincentives. This directly addresses RFI question PR-12, which asks about revising Information Blocking exceptions; this practice should not qualify for any exception, as it does not serve any legitimate purpose that is not already satisfied by the natural incentives in the ecosystem and existing privacy regulations that govern third-party apps.

Justification and Alignment with CMS Goals: This recommendation is essential to protect the patient's central role in controlling their own health data, a core tenet of the Cures Act. It directly addresses CMS's concern that the current patient experience is "neither seamless nor simple" and is critical to promoting a competitive, innovative app marketplace where success is determined by value to the patient, not by the business preferences of an EHR vendor.[1] Failure to regulate this behavior signals to the market that the "rules" of interoperability can be bent by powerful incumbents, creating a massive disincentive for the very investment and innovation CMS seeks to cultivate. Regulating the authorization workflow is therefore not just about user experience; it is about ensuring the fundamental economic viability of the third-party app ecosystem.

Subsection 2.3: Mandating Efficient, Scalable Data Access with Bulk FHIR and Subscriptions

RFI Questions Addressed: TD-1, TD-2, TD-10, TD-13, TD-15, TD-16, PR-4

Issue Identification: The current Patient Access API framework mandates a data access paradigm that is architecturally primitive and fundamentally unsustainable at scale. It requires applications to retrieve a patient's record one resource at a time through a series of complex, iterative, and paginated API requests. This polling-based model imposes a massive and duplicative engineering burden on every application developer and, as adoption of patient apps becomes widespread, could create an immense, unnecessary, and ultimately crippling performance load on provider and payer servers.

Real-World Impact Analysis: Application developers are forced to spend a disproportionate amount of their resources building and maintaining brittle, vendor-specific data-fetching logic, diverting effort away from creating the value-added features for patients that CMS wishes to encourage.

To maintain data freshness, applications must periodically re-poll and re-import a

patient's entire record, often on a weekly basis. This is grossly inefficient, as the vast majority of the data is unchanged. As the digital health ecosystem grows, with millions of patients using dozens of apps, this constant, high-volume polling will lead to systemic performance degradation and a potential collapse of the infrastructure intended to support it. The current architecture is not just inefficient; it could be at risk of failure under the load of its own success.

Proposed Solution: CMS must mandate a transition to the modern, event-driven, and bulk-capable data access paradigm already in use by other stakeholders in the ecosystem by requiring support for patient app access to two existing, mature HL7 FHIR standards.

1. **Mandate Patient-Authorized Bulk FHIR Access:** Require all Certified Health IT to support the **HL7 FHIR Bulk Data Access Implementation Guide (v2.0.0)** for single-patient contexts.[2] This is a critical distinction: we are not requesting population-level access, but rather the application of this existing, powerful standard to the patient-authorized use case. With this mandate, an authorized application could make a single API call to initiate an asynchronous export of a single patient's complete Electronic Health Information (EHI), as defined under USCDI v3 and the FHIR Patient Compartment. The server would then prepare a collection of files (e.g., one for all conditions, one for all medications) and provide the app with a secure link to download them. This replaces thousands of individual API calls with a single, efficient transaction.
2. **Mandate FHIR Subscriptions for Third-Party Apps:** Require all Certified Health IT to make their FHIR Subscription capabilities available to authorized third-party applications. This is essential for providing applications with real-time notifications of clinical events (e.g., a new lab result is available, a patient has been admitted to the hospital) without wasteful polling. The technical foundation for this already exists, as many major EHR vendors use this functionality for their own internal purposes.[1] The mandate should specify adherence to the principles in the **FHIR R5 Subscriptions framework**, which can be implemented in FHIR R4 via the official **HL7 FHIR Subscriptions R5 Backport Implementation Guide**.[4] This provides a clear, standards-based path for implementation.

Justification and Alignment with CMS Goals: This dual mandate directly addresses the RFI's call to "reduce barriers to data access" and "realize the potential of recent innovations".[1] It dramatically reduces the technical burden on developers (TD-1), improves the timeliness and quality of data available to patients (PC-5b), and creates a scalable, resilient infrastructure that can support a thriving application ecosystem without overwhelming provider systems. This is a form of "future-proofing" the national

health IT infrastructure, representing a proactive investment in a sustainable architecture rather than a reactive patch to a failing one. By lowering the technical barrier to entry, this policy would also foster greater competition and diversity among application developers, particularly benefiting smaller innovators and startups.

Subsection 2.4: Expanding Data Access Beyond USCDI for Meaningful Clinical Utility

RFI Questions Addressed: TD-2, TD-7, TD-10, TD-13

Issue Identification: While the United States Core Data for Interoperability (USCDI) standard provides a crucial baseline for interoperable data exchange, limiting patient-authorized API access to *only* the data elements within USCDI severely constrains the clinical utility and innovative potential of third-party applications.

Real-World Impact Analysis: The value of a digital health application is directly proportional to the comprehensiveness of the data it can access. An application designed to help a patient manage post-operative care is of limited use without access to the full details of the hospital stay (via $Encounter), or information about scheduled follow-up visits (via $Appointment). An app for a cancer patient is hamstrung without access to the full pathology reports and imaging studies. Limiting data access to a small subset of data elements leaves the majority of the patient's clinical story locked away, relegating most apps to the role of simple data viewers rather than active partners in care management.

Proposed Solution: In alignment with the 21st Century Cures Act's clear intent to provide patients with access to all of their EHI, CMS and ONC must clarify that the Patient Access API mandate extends beyond the confines of the current USCDI version.

- Specifically, CMS should require certified systems to make the following additional FHIR resources available through the Patient Access API upon patient authorization, as they contain data essential for a wide range of high-value health management and care navigation use cases:
    - $ImagingStudy: To access diagnostic imaging reports and metadata.
    - $Encounter: To provide the contextual glue of hospital admissions, emergency department visits, and outpatient appointments.
    - $Appointment and $AppointmentResponse: To enable applications that help

patients manage their scheduled care.

Justification and Alignment with CMS Goals: This recommendation directly addresses RFI question TD-13 regarding the opportunities that could emerge with access to the entirety of a patient's EHI. By unlocking these additional data types, CMS would enable a new generation of more sophisticated and clinically valuable applications. This move is essential to transition the ecosystem from basic data access to meaningful data *use*, thereby improving health outcomes, supporting chronic disease management, and empowering patients to be more active participants in their own care.

Subsection 2.5: Strengthening Ecosystem Reliability and Developer Support

RFI Questions Addressed: TD-2, TD-10, TD-18, PR-3, PR-4

Issue Identification: The current digital health ecosystem lacks the basic, professional-grade support infrastructure expected of any mission-critical IT system. When a provider's FHIR API fails or returns errors, third-party developers have no reliable channel to report the issue or receive updates on its resolution. Furthermore, when bugs or non-conformant behaviors are discovered in a certified product's API, the reporting process is fragmented, opaque, and in some cases, requires developers to enter into paid agreements simply to view the EHR vendor’s developer forum or file a bug report in the tracking system that they actually monitor.

Real-World Impact Analysis: This operational immaturity creates a brittle and untrustworthy ecosystem. API outages can persist for days or weeks, leaving patients unable to access their data and developers powerless to help them. Critical bugs that affect thousands of patients can be ignored or swept under the carpet by vendors who control their own siloed, private bug-tracking systems. This lack of transparency and accountability erodes developer and user confidence and signals that the interoperability framework is not yet being treated as the production-grade, life-critical infrastructure that it is.

Proposed Solution: CMS must mandate the implementation of two key support structures to professionalize the ecosystem and ensure a baseline level of operational reliability.

1. **Mandatory, Monitored Technical Contacts:** Require all Certified Health IT developers to populate the $Endpoint.contact element in the FHIR

CapabilityStatement for every production endpoint. This field must contain a valid email address or service desk portal URL that is actively monitored by a responsible party capable of addressing technical issues. Acknowledgment of receipt of an issue should be automated, and a response from a human should be guaranteed within a defined period, such as two business days. Failure to provide or maintain this monitored contact channel should be considered a form of information blocking.

2. **Centralized, Public Bug Reporting Platform:** CMS, in partnership with ONC, should establish and manage a single, public platform for reporting and tracking bugs, implementation errors, and conformance issues with certified APIs. This platform would function like an open-source issue tracker (e.g., a public GitHub repository).
    - **Transparency:** All submitted issues and vendor responses would be public, fostering collaboration and preventing the duplication of effort.
    - **Accountability:** Certified Health IT vendors must be required to publicly acknowledge and provide status updates on reported issues affecting their products within a fixed timeframe (e.g., 90 days). Failure to respond in a timely and substantive manner should create a presumption of information blocking, triggering investigation and potential disincentives.

Justification and Alignment with CMS Goals: These low-burden, high-impact solutions would dramatically improve the stability, reliability, and transparency of the entire interoperability ecosystem. They foster a collaborative environment, reduce wasted effort across the developer community, and hold vendors accountable for the quality and performance of their certified products. This directly supports the CMS goal of ensuring that data is not only available but also timely and reliable, which is essential for building patient trust and enabling a scalable health system.

Subsection 2.6: Streamlining Patient Access Through Standardized Digital Identity

RFI Questions Addressed: PA-3, TD-3, PR-9, PC-14

Issue Identification: The current digital identity landscape in healthcare is a significant and unnecessary barrier to patient data access. Patients are forced to create and manage a separate, proprietary set of login credentials for each provider's patient portal and each health plan's member portal. As noted in the RFI, this proliferation of usernames and passwords leads to significant "credential fatigue," causing patients to

forget passwords, abandon attempts to access their data, and struggle to use applications that could aggregate their health information from multiple sources.

Real-World Impact Analysis: A patient trying to use a health management app to get a complete view of their health might need to remember and successfully enter a dozen different login credentials for their primary care physician, various specialists, the local hospital, and their Medicare Advantage plan. This friction-filled process is a major deterrent to engagement and directly undermines the goal of providing patients with a simple, consolidated view of their health information.

Proposed Solution: CMS should mandate that all patient-facing applications and associated FHIR API endpoints regulated under its authority support authentication via trusted, third-party digital identity credentials.

- **Leverage Existing Standards:** The mandate should require support for credentials that meet the federal government's own standards for security and trust: **NIST Special Publication 800-63-3 Identity Assurance Level 2 (IAL2) and Authenticator Assurance Level 2 (AAL2)**.
- **Utilize Trusted Providers:** This would allow patients to use a single, secure, and portable identity from an existing, trusted Credential Service Provider (CSP) — such as **Login.gov** or **ID.me** — to access their health information across the entire ecosystem.
- **Clarify Scope:** It is critical to note that this recommendation is aimed squarely at simplifying **patient-facing login and authentication workflows**. It is not a proposal to change requirements for clinical or administrative identity proofing within a healthcare facility. The goal is to solve the patient's credential management problem.

Justification and Alignment with CMS Goals: This proposal directly addresses the suite of RFI questions on digital identity (PC-14, PR-9, PA-3, TD-3). By creating a consistent, portable, and secure identity layer, CMS would dramatically simplify the patient experience, reduce a major barrier to the adoption of digital health tools, and enable the most valuable care navigation and health management use cases which require data aggregation from multiple providers and payers. This is a critical step toward making the vision of a single, patient-controlled health record a practical reality.

Subsection 2.7: Aligning Incentives and Enforcement to Drive Adoption

RFI Questions Addressed: PA-2, PR-12, TD-18

Issue Identification: Regulatory mandates, while essential, are often insufficient on their own to drive timely and good-faith implementation by entrenched market actors. Experience across multiple industries has shown that policies must be coupled with strong financial incentives and clear, robust enforcement mechanisms to overcome market inertia and resistance. The slow, inconsistent, and often non-conformant rollout of implementations against existing interoperability rules demonstrates this reality in healthcare.

Real-World Impact Analysis: Without clear consequences, payers may delay API implementation, and EHR vendors may engage in the types of subtle information blocking practices detailed throughout this response (e.g., scare screens, non-public/pay-to-play developer forums, unmonitored endpoints). This results in a stalled ecosystem where the promise of policy outpaces the reality of implementation, leaving patients and innovators waiting for the access mandated by law.

Proposed Solution: CMS must use its powerful policy levers to create unambiguous incentives for compliance and disincentives for non-compliance.

1. **Tie API Adoption Among Payers to Medicare Advantage Payment:** To directly address the slow pace of payer API implementation (RFI Question PA-2), CMS should condition a meaningful portion of Medicare Advantage (MA) capitated payments on full, demonstrable compliance with all Patient, Provider, and Payer-to-Payer Access API requirements. Compliance should not be a simple check-box, but should be validated against the technical and operational enhancements proposed in this response, including support for the National Provider-to-FHIR Endpoint Directory, Bulk FHIR, and FHIR Subscriptions. Given that most major payers derive significant revenue from MA, this will immediately elevate API implementation to a top-tier business priority.
2. **Expand and Enforce the Definition of Information Blocking:** CMS and ONC should issue joint guidance that explicitly clarifies that the technical and procedural failures detailed in this response constitute practices that interfere with the access, exchange, or use of EHI and are therefore subject to Information Blocking disincentives (RFI Questions PR-12, TD-18). These practices should include, but not be limited to:
    - The use of "scare screens" or other manipulative authorization workflows.
    - Failure to publish and maintain accurate data in the National Provider-to-FHIR Endpoint Directory.
    - Failure to provide and monitor a technical contact channel for a certified API

endpoint.
    - Failure to respond to issues on the centralized public bug reporting platform within the defined time period.
    - Failure to provide access to Bulk FHIR and FHIR Subscription capabilities to authorized patient apps.

Justification and Alignment with CMS Goals: These recommendations provide the necessary "teeth" to ensure that the technical mandates proposed in this document are prioritized and implemented in good faith. Financial incentives and clear, swift enforcement actions are the most effective tools CMS possesses to overcome market resistance and ensure that the letter and spirit of the law are fulfilled. This approach transforms interoperability from a compliance exercise into a core business imperative, aligning the interests of all stakeholders with the ultimate goal of empowering patients.

Section III: Conclusion

Unite commends the Centers for Medicare & Medicaid Services and the Assistant Secretary for Technology Policy/Office of the National Coordinator for Health Information Technology for their unwavering commitment to building a modern, interoperable, and patient-centered healthcare system. The policy framework established to date has been instrumental in initiating this transformation. However, to move from foundational principles to a functional, seamless reality for patients, the next phase of rulemaking must be precise, technical, and decisive.

The recommendations detailed in this response are not a menu of discrete options but an integrated, interdependent roadmap for systemic improvement. A National Provider-to-FHIR Endpoint Directory is of little use if the endpoints themselves are unreliable and the data behind them is incomplete. Efficient data access patterns like Bulk FHIR and Subscriptions cannot be leveraged if patients are deterred from authorizing apps by manipulative "scare screens." The entire ecosystem cannot scale without robust support infrastructure and a consistent approach to digital identity. And none of these technical advancements will be prioritized by incumbent actors without clear financial incentives and vigorous enforcement of the rules.

By adopting this comprehensive set of recommendations, CMS and ONC can dismantle the most significant remaining barriers to interoperability. These actions will foster a truly competitive and innovative market for digital health applications, reduce

administrative burden, and dramatically improve the stability and reliability of our national health IT infrastructure. Most importantly, they will finally deliver on the central promise of the 21st Century Cures Act: to enable a patient-centric learning health system and provide all Americans with simple, secure, and meaningful control over their own health information.

We thank you again for the opportunity to provide these comments and stand ready to serve in any capacity as you continue this vital work.

Sincerely,

Taner Dagdelen
Chief Executive Officer
Unite

Works cited

- Centers for Medicare & Medicaid Services. "Request for Information: National Standards for the Exchange of Electronic Health Information." *Regulations.gov*, comment CMS-2025-0050-0031, accessed June 16, 2025. https://www.regulations.gov/document/CMS-2025-0050-0031
- "The FHIR Bulk Data API and What's New!" *DevDays*, accessed June, 2025. https://www.devdays.com/wp-content/uploads/2024/07/6.10.24-Dan-Gottlieb-The-FHIR-Bulk-Data-API.pdf
- "Home - Bulk Data Access IG v2.0.0 - FHIR specification." *HL7*, accessed June, 2025. https://build.fhir.org/ig/HL7/bulk-data/
- "HL7.FHIR.UV.SUBSCRIPTIONS-BACKPORT\Home - FHIR v4.1.0." *GitHub Pages*, accessed June, 2025. https://argonautproject.github.io/subscription-backport-ig/
- "Subscriptions Test Kit - Inferno." *HealthIT.gov*, accessed June, 2025. https://inferno.healthit.gov/test-kits/subscriptions/