ConnectedHealthInitiative

June 16, 2025

Robert F. Kennedy, Jr.
U.S. Secretary of Health and Human Services
200 Independence Ave. Southwest
Washington, DC 20201

RE: ***Comments of the Connected Health Initiative,*** **Request for Information; Health Technology Ecosystem** ***[CMS-0042-NC; RIN 0938-AV68]***

The Connected Health Initiative[1] represents stakeholders from across the healthcare community who share your goals of driving the development and adoption of digital health management and care navigation applications and strengthening interoperability and secure access to health data through open, standards-based technologies. We appreciate the opportunity to respond to your Request for Information[2] regarding the market of digital health products for Medicare beneficiaries as well as the state of data interoperability and broader health technology infrastructure. We are committed to increasing beneficiary access to effective digital capabilities needed to make informed health decisions and increasing data availability for all stakeholders contributing to health outcomes.

Support for digital health innovations across the healthcare continuum are important and lifesaving for patients. A truly interoperable healthcare system facilitates patient engagement across a range of modalities with open application programming interfaces (APIs) that allow the safe and secure introduction of patient-generated health data (PGHD) into electronic health records (EHRs). Data stored in standardized and structured formats with interoperability facilitated by APIs provides analytics as well as near real-time alerting capabilities. The efficacy of precision medicine, population health, and clinical decision support – all critical means for combatting chronic diseases – is dependent in large part on the availability of data.

We emphasize the linkage of ensuring interoperability to the Administration's priorities described in the RFI, including leveraging the tremendous potential of artificial intelligence (AI). Many AI use cases, ranging from solving administrative/backend efficiencies to supporting clinical decisions, have already begun to emerge as necessary to advancing the Quadruple Aim. Bold policies will be needed if AI is to positively transform the American healthcare system.

CHI provides detailed answers to a wide range of questions posed in the RFI. Key themes and recommendations we make include:

- **HHS should improve access, usability, and trust in digital health products through expanded use of secure and standardized APIs for real-time data sharing**, supporting adoption by payers and providers to improve care coordination and empower patients.

[1] www.connectedhi.com.
[2] 90 FR 21034.

- **HHS should take numerous concrete steps across the department to improve access to effective digital capabilities and increase data availability for all stakeholders contributing to health outcomes.** In the most immediate, the Department of Health and Human Services should take steps to end information blocking practices that are actively harming patients, with a focus on health IT developers who view information blocking as a competitive advantage.
- **HHS should take overdue steps to bring the power of digital health tools, including AI, into care through overdue reforms to payment and incentive policies.** Needed steps include revising CMS' practice expense methodology to better support Software as a Medical Device (SaMD) and better integrate telehealth, remote monitoring, and AI into Medicare services; and focus on outcome-based approaches in the Quality Payment Program in welcoming the use of digital health tools. HHS should also align evidentiary standards for clinical evidence across the agency to streamline access to innovative AI-enabled tools and ensure consistent evaluation for safety, efficacy, and real-world impact.
- **HHS should act rapidly to realize the potential of artificial intelligence (AI) which will improve healthcare, prevent hospitalizations, reduce complications, and improve patient engagement.** CHI has worked to proactively address health AI governance and policy issues based on consensus views that span the healthcare sector, from technology developers to providers to patients, and urge for alignment with CHI's Health AI Policy Principles; CHI recommendations on advancing transparency for AI in the healthcare ecosystem; CHI's AI Roles and Interdependencies Framework; and CHI's recommendations to the Department on Government Efficiency on ways to use AI to improve healthcare governance efficiency.
- **HHS should focus on fully leveraging digital health tools in achieving value-based care goals.** Value-based care goals simply cannot be accomplished without embracing the efficiencies digital health tools offer given their demonstrated ability to advance the Quadruple Aim.
- **HHS should take proactive steps to combat the growing impact of standard essential patent (SEP) licensor abuses on the digital healthcare sector**, ensuring that standards-based abuses by SEP holders do not undermine the Administration's goal of creating a competitive and open healthcare technology ecosystem.
- **HHS should enhance accessibility and digital literacy by engaging in educational support and community outreach**, especially among the patient community. HHS' role, in partnership with technology developers, providers, and payers, is critical in supporting the responsible uptake of digital health tools across the country.

Across all of our recommended actions, coordination across HHS, and the federal government and states, will be critical to accomplishing meaningful improvements to the U.S. health technology ecosystem.

We again express our support for the Administration's commitment to increasing beneficiary access to effective digital capabilities needed to make informed health decisions, and increasing data availability for all stakeholders contributing to health outcomes. Our community welcomes the opportunity to meet with you to discuss our shared views.

Sincerely,

Brian Scarpelli
Executive Director

Chapin Gregor
Policy Counsel

Connected Health Initiative
1401 K St NW
Suite 501
Washington, DC 20005

CC: **Dr. Thomas Keane, Assistant Secretary for Technology Policy, National Coordinator for Health Information Technology**

Dr. Mehmet Oz, Administrator, Centers for Medicare & Medicaid Services

Dr. Jay Bhattacharya, Director, National Institutes of Health

Christi Grimm, Inspector General, Office of Inspector General

Amy Gleason, Administrator, United States DOGE Service

ConnectedHealthInitiative

Responses of the Connected Health Initiative –

Request for information; Health Technology Ecosystem

90 FR 21034

Table of Contents

Patients and Caregivers

1. Patient Needs

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

CMS and its partners can encourage patient and caregiver interest in health management and care navigation apps by expanding access, enhancing usability, and building trust in digital tools. Additionally, CMS and its partners can help foster greater patient and caregiver engagement with health management and care navigation apps by prioritizing interoperability, data security, and consumer-focused design. CMS should also seek consistent stakeholder input on ways to better leverage technology for patient engagement, incentives for app use, educational campaigns, and integration of digital health tools into routine care as collaboration with the private sector is central to developing user-friendly, secure apps that meet the needs and preferences of diverse patient populations.

CMS is encouraged to actively invest in foundational infrastructure such as a dynamic, interoperable national provider directory, modern identity verification, and expanded patient access APIs, all of which make it easier for patients and caregivers to securely access and manage their health information through apps. The agency's new strategic direction should also emphasize consumer engagement and evidence-based prevention, aiming to empower individuals with the data and tools they need to make informed health decisions.

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 can play a valuable role in encouraging the adoption of digital health products by evaluating their real-world impact on health care quality and outcomes, especially for Medicare and Medicaid beneficiaries. Rather than duplicating the FDA's safety oversight, CMS could focus on how these tools improve patient experience, clinical outcomes, usability, accessibility, and interoperability with existing health IT systems. Criteria for such a review might include evidence of improved outcomes, ease of use for diverse populations, data security, and the ability to reduce provider and patient burden without worsening disparities.

To boost adoption among patients and caregivers, CMS could expand access to health data through secure APIs, adjust reimbursement models to reward effective digital tools, and invest in education campaigns that build trust and digital literacy. Encouraging user-centered design and supporting partnerships with community organizations would further help ensure that digital health solutions are accessible, effective, and widely used in value-based care.

CMS has previously proposed it may conduct an "Evidence Preview" to identify gaps in the evidence required to achieve the "reasonable and necessary" criteria for a National Coverage Decision. The applicant may then offer an "Evidence Development Plan" as the basis for the clinical trials program to satisfy the CED requirement to qualify for TCET - as well as any post-market requirements of the FDA. By requiring CED as a condition of providing coverage with immediate effect from FDA clearance/approval, TCET compresses the continuum across FDA to CPT to CMS in anticipation of the evidence to support "Reasonable and Necessary" above and beyond FDA's "Safety and Efficacy" (balance of benefits and harms).

In order for CED to begin with immediate effect from FDA clearance, CMS must engage the innovator and FDA to agree the protocol design supplemental to the FDA's requirements, prior to FDA clearance of the product and, therefore, in parallel with FDA's deliberations of final labeling and any post-market requirements. These decisions will be of particular importance because many of the products qualifying for Breakthrough Designation, and therefore also for TCET, would represent new predicate devices.

The evidentiary standard required by FDA would represent the baseline from which the evidentiary standard for CMS would be achieved. Any post-marketing requirements of FDA's could be achieved in the CED trials. A common understanding and description of the output from these devices, as represented by the AI Taxonomy in CPT Appendix S, would anchor this continuum. The descriptors Assistive, Augmentative, and Autonomous, as they apply to the output of these devices, are rigorously and consistently applied in the creation of new reimbursement codes consistent with the clinical evidence supporting their meaningfulness. By harmonized use of these same descriptors in FDA labeling and CMS coverage policy, each would have its own set of progressively developed and synchronous evidentiary standards based on a shared understanding of the impact of the output, thus avoiding mis-alignment among labeling, coding, valuation, and coverage.

In CPT coding, "clinically meaningful" refers to the output from a procedure or service. The output must be sufficiently well validated [clinically, as distinct from technically] that, in the judgement of a prudent physician or other qualified health professional, it is likely to contribute directly to decision-making for an individual patient's care pathway leading to a beneficial outcome. The use of the term "Clinically Meaningful" is also synchronous with FDA's requirements for clearance/approval of AI/ML. As an example, the Guidance for Quantitation requires that the manufacturer provide sufficient information that the practitioner understands how to use the output in patient care; this too is consistent with the CPT requirement for Augmentative.

To qualify for these terms in a CPT code, validation of the output, as documented in medical literature and clinical practice guidelines or FDA-cleared or -approved labeling, may be achieved by:

1. Direct association with clinically meaningful differences in outcomes, similarly as characterized by CMS and AHRQ in the Evidence Development Plan, CED Guidance, and NCA Evidence Review; or
2. Correlation with the output from another procedure or service which is currently considered "usual care" because it has been proven to contribute directly to clinically meaningful differences in outcome.

In CMS's proposals for TCET and CED, this term "clinically meaningful" is used as a standard for the outcome metrics and the statistical analysis plans for the clinical trials. It is distinct from closely related terms such as "Medically Necessary" as judged by CMS in determining coverage policy, "Clinically Valid" as judged by FDA in determining balance of harms and benefits for market entry, and "equipoise" as used by IRBs in adjudicating the ethics of clinical experimentation.

In the Evidence Development Plan, in order to sufficiently address evidence gaps identified by CMS and AHRQ in the Evidence Preview, the applicant is required to include *clinically meaningful benchmarks for each study outcome*. Designing the trial for CED in consultation with CMS and AHRQ to meet the Objective Success Criteria, the applicant must establish an evidentiary threshold for the primary *outcome to demonstrate clinically meaningful differences and adequate numbers of subjects to* achieve the precision necessary for *values that indicate a meaningful effect*. Finally, the proposed National Coverage Assessment Evidence Review (to provide a framework for more predictable and transparent evidence development) stipulates that an intervention's *benefits should generally be clinically meaningful*, characterizing "strong evidence from clinical trials" including those which may have been published during the period of CED, include adequate numbers of patients to demonstrate improvement in outcomes which are not only statistically significant but also *clinically meaningful.* A current example can be found in CMS' requirements for clinical studies of a monoclonal antibody directed against amyloid approved by FDA, which include that they adhere to the standards of scientific integrity that have been identified by AHRQ (i.e., that the principal purpose of the study is to test whether the *item or service meaningfully improves health outcomes* of affected beneficiaries represented by the enrolled subjects). These uses of the term "clinically meaningful" are aligned with those of CPT, and synchronous in setting standards for clinical evidence.

In summary, synchrony on the evidentiary standards and alignment on the impact of output across FDA, CPT, and CMS will streamline access to the benefits of AI/ML in medicine. Harmonious utilization of the descriptors in CPT Appendix S, such as Augmentative and Autonomous, will contribute to this synchrony in the evidentiary standards, for example as reflected in the requirement for "clinical meaningfulness" in CPT coding and CMS coverage. CMS should encourage this in the TCET program; alignment on the impact of output, for example as reflected in the criteria for Breakthrough Designation and TCET, will ensure the most necessary innovation will be brought to bear on patient outcomes, most expeditiously.

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

To enable timely access to high quality CMS and provider generated data on patients, CMS should expand the use of secure, standardizes APIs, such as those based on FHIR and USCDI, which allow real-time sharing of claims, clinical, and prior authorization data.

By requiring both payers and providers to adopt these technologies, CMS ensures that patients, clinicians, and authorized apps can easily access and use comprehensive health information. Standardizing data elements and making provider directories available through public-facing APIs further streamlines care coordination and network identification. These steps, combined with clear

implementation guides and strong patient data-sharing controls, make it easier for all parties to access reliable, up-to-date health information, ultimately improving care quality and efficiency.

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?

To make digital health products accessible and easy to use for Medicare beneficiaries and caregivers several key features are essential. Please see the following recommendations:

First, products must incorporate digital accessibility principles, including plain language content, adjustable text sizes, keyboard-only navigation, and compatibility with assistive technologies like screen readers to accommodate vision, hearing, cognitive, and physical impairments common among older adults.

Second, creating an intuitive, user-friendly design with simple navigation and clear instructions helps reduce barriers for users unfamiliar with technology. Providing **actionable, plain language information** empowers beneficiaries to engage confidently with their health data and care management tools.

Third, ensuring secure but straightforward access, such as through streamlined identity verification and integration with familiar platforms, can build trust and ease onboarding. CMS's efforts to expand patient access APIs and develop digital insurance cards aim to simplify access to health information in real time, further supporting usability.

Finally, implementing educational support and outreach tailored to seniors and caregivers, such as tutorials, help lines, and community partnerships, are crucial to increasing digital literacy and encourage adoption.

Together, these features help create digital health products that are inclusive, trustworthy, and empowering for Medicare beneficiaries and their caregivers.

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?

The best way for CMS to collect real-world data on digital health products' impact on health outcomes and costs is to use a standardized, transparent protocol that draws from diverse data sources such as electronic health records, claims, registries, and device-generated information. CMS is already moving in this direction with the proposed HARPER+ protocol template, which aligns with FDA guidance and sets out clear requirements for real-world data (RWD) studies. This approach ensures that data collection is consistent, reproducible, and relevant to Medicare populations.

Additionally, CMS can leverage its existing administrative databases and facilitate pragmatic trials embedded in health insurance plans, which provide longitudinal data on patient demographics, treatments, and outcomes. By integrating these data sources and using standardized methods, CMS can efficiently monitor digital health products after market release, assess their real-world effectiveness and safety, and evaluate their impact on healthcare costs.

Public feedback and stakeholder engagement in refining these protocols will further strengthen the quality and utility of the evidence collected, ultimately supporting better decision-making and improved patient outcomes.

2. Data Access and Integration

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)?**

Valuable data that remains difficult for patients, caregivers, app developers, and technical vendors to access includes claims data, detailed clinical data (such as encounter notes and operative reports), appointment schedules, and price transparency information. Barriers stem from technical limitations, lack of standardized systems, privacy and security concerns, and cumbersome permission processes that often require repeated HIPAA forms or provider-driven controls rather than patient empowerment.

Patients and caregivers frequently face challenges accessing comprehensive health records and imaging results, while app developers struggle with inconsistent data formats, limited interoperability, and restricted access to real-time or granular clinical data. Additionally, privacy concerns and a lack of trust in how data will be used or shared further inhibit willingness to share or access valuable health information.

Overcoming these barriers will require more patient-centered permission processes, harmonized data standards, and transparent privacy protections to ensure that critical health data is accessible for appropriate and beneficial use across the healthcare ecosystem.

b. **What are specific sources, other than claims and clinical data, that would be of highest value, and why?**

Beyond claims and clinical data, several other data sources are highly valuable for improving patient care, outcomes research, and health system performance, yet are often underutilized or difficult to access:

- **Social Determinants of Health (SDOH) Data:** Information on factors like housing, income, education, food security, and environment are critical for understanding patient risk and tailoring interventions, as these factors significantly influence health outcomes.
- **Behavioral and Lifestyle Data:** Data on physical activity, diet, tobacco and alcohol use, and mental health status provide important context for preventive care and chronic disease management. These data points are often collected through public health surveys or digital health tools.
- **Public Health Surveillance and Environmental Data:** Sources such as the CDC's Behavioral Risk Factor Surveillance System (BRFSS), National Environmental Public Health Tracking Network, and disease-specific registries offer insights on population health trends, risk factors, and exposures that can inform care strategies.
- **Vital Statistics:** Mortality, birth, and cause-of-death data from systems like the CDC's National Vital Statistics System are essential for tracking outcomes and understanding health trends at the population level.
- **Patient-Reported Outcomes and Experience Data:** Information directly from patients about their symptoms, quality of life, and satisfaction with care can provide a more complete picture of treatment effectiveness and patient needs.
- **Appointment Schedules and Provider Availability:** Real-time access to provider schedules and appointment slots can improve care coordination and timely access. Unfortunately, this is often siloed within provider systems.
- **Price and Cost Transparency Data:** Data on the prices of services, out-of-pocket costs, and coverage details empower patients and caregivers to make informed decisions but remain challenging to access in a user-friendly, actionable format.

These sources, when integrated with claims and clinical data, offer a more holistic view of patient health and care delivery, enabling more personalized and effective interventions.

c. What specific opportunities and challenges exist to improve accessibility, interoperability and integration of clinical data from different sources to enable more meaningful clinical research and generation of actionable evidence?

Though, efforts to improve accessibility and interoperability of clinical data are advancing, especially with the enforcement of information blocking rules that impose significant penalties on health IT developers and exchanges that restrict data sharing, challenges persist. There is ongoing uncertainty regarding compliance and exceptions to the rules because enforcement for healthcare providers is still being finalized. Technical barriers, such as inconsistent data formats and integration difficulties, further complicate seamless data sharing. Additionally, some organizations remain hesitant to share data due to privacy concerns or competitive interests. While regulatory progress is creating new opportunities for data-driven research, overcoming these technical, cultural, and policy hurdles will be essential to fully realize the promise of integrated clinical data.

Further, CHI has worked to proactively address health AI governance and policy issues based on consensus views that span the healthcare sector, from technology developers to providers to patients, and we urge for alignment with:

- The CHI community's Health AI Policy Principles (https://connectedhi.com/wp-content/uploads/2022/02/Policy-Principles-for-AI.pdf);
- CHI recommendations on advancing transparency for AI in the healthcare ecosystem (https://connectedhi.com/wp-content/uploads/2022/02/AdvancingTransparencyforArtificialIntelligenceintheHealthcareEcosystem.pdf);
- CHI's AI Roles and Interdependencies Framework (https://connectedhi.com/wp-content/uploads/2024/02/CHI-Health-AI-Roles.pdf); and
- CHI's recommendations to the Department on Government Efficiency on ways to use AI to improve healthcare governance efficiency (https://connectedhi.com/wp-content/uploads/2025/01/CHI-DOGE-Recommendations-30-Jan-2025.pdf).

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?

CHI community members consistently identify several additional CMS data sources as highly valuable for inclusion in the Blue Button 2.0 API to enable more useful digital products for patients and caregivers. Beyond the current scope of basic demographics, Medicare coverage, and claims data (Parts A, B, and D), the most requested enhancements include:

- **Clinical Data from EHRs:** Access to clinical records such as lab results, diagnoses, medications, immunizations, allergies, encounter notes, and operative reports would provide a much fuller picture of patient health and care history, supporting better care management and coordination.
- **Encounter and Provider Data:** Detailed information on healthcare encounters, including provider names, specialties, locations, and appointment histories, would help patients and caregivers track care episodes and coordinate follow-up.
- **Price and Cost Transparency Data:** Real-time access to service prices, out-of-pocket costs, and coverage details would empower beneficiaries to make informed decisions about their care and financial planning.
- **Prior Authorization and Coverage Decisions:** Including data on prior authorizations, denials, and appeals would help patients and caregivers understand and navigate insurance processes more effectively.
- **Appointment Schedules and Availability:** Integration of appointment scheduling and provider availability would facilitate timely access to care and improve patient engagement.

- **Social Determinants of Health (SDOH):** Data related to housing, transportation, food security, and other social factors would enable more personalized and holistic care planning.

Expanding the Blue Button 2.0 API to encompass these data types would significantly enhance the utility of digital health tools for Medicare beneficiaries and their caregivers, supporting better decision-making, care coordination, and health outcomes.

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

a. **Please provide specific examples.**
b. **What changes would you suggest?**
c. **What use cases could have a significant impact if implemented through TEFCA?**
d. **What standards are you aware of that are currently working well to advance access and existing exchange purposes?**
e. **What standards are you aware of that are not currently in wide use, but could improve data access and integration?**
f. **Are there redundant standards, protocols, or channels that should be consolidated?**
g. **Are there adequate alternatives outside of TEFCA for achieving widespread patient access to their health information?**

TEFCA (Trusted Exchange Framework and Common Agreement) introduces several unique interoperability functions that set it apart from previous efforts to connect healthcare data nationwide, ultimately advancing provider access. However, TEFCA's implementation is not without its challenges. As we have noted on the record before, a proposed reliance on TEFCA could privilege licensed health care providers and exclude all other providers of healthcare services in creating a two tiered system where providers who are subject to federal privacy and security laws but are not licensed health care professionals as defined in TEFCA Standard Operating Procedures will have to undertake actions above and beyond those taken by licensed health care providers to ensure that their queries for patient health information for treatment are responded to and not blocked. The creation of such a dynamic is counter to the Cures Act requirement that "special effort" not be required.[1] In addition, by artificially siloing data from digital-first health care providers, the proposed rule severely hampers the access, exchange, and use of a growing subset of electronically accessible health information by the full ecosystem of providers in the interest of patients, as we'll discuss below regarding impact.

Notably, TEFCA has the potential to facilitate access to comprehensive, standardized clinical information spanning various healthcare environments and regions for AI-driven applications. Despite this promise, availability of such data remains constrained. Typically, developers must collaborate with TEFCA-affiliated organizations, such as hospitals or health networks, and are restricted to using the information for specific functions, most often related to care delivery, billing, or administrative tasks. Broader applications, including the creation of AI algorithms, are generally

[1] 21st Century Cures section 4002, adding 42 USC 300jj-11(D)(iv)

not allowed under existing policies unless the data is anonymized or explicit patient consent is obtained. Future revisions to the framework could consider ways to responsibly broaden the range of acceptable uses.

- **Nationwide Network-to-Network Connectivity:** TEFCA establishes a "network of networks" model, which envisions Qualified Health Information Networks (QHINs) connecting directly to each other, enabling seamless, secure exchange of electronic health information (EHI) across the country, regardless of the underlying technology or vendor.
- **Common Rules of the Road:** All participating Health Information Networks (HINs) and their members are bound by a single set of legal, technical, and operational requirements. This includes standardized authentication, authorization, privacy, and security policies, reducing fragmentation and simplifying participation.
- **Standardized Technical Framework:** The QHIN Technical Framework (QTF) specifies core interoperability functions such as certificate policy, secure channels, mutual authentication, user authentication, authorization, patient identity resolution, record location, directory services, privacy preferences, auditing, and error handling. These standards enable advanced functions like broadcast queries, targeted queries, and message delivery between QHINs.
- **Support for Multiple Exchange Purposes:** TEFCA is designed to support a broad range of use cases, including treatment, individual access, payment, healthcare operations, and public health, expanding beyond the limited purposes of earlier networks.
- **Governance and Oversight:** TEFCA provides a governance structure, including minimum required terms and conditions (MRTCs), additional required terms and conditions (ARTCs), and standard operating procedures (SOPs) to ensure compliance and resolve disputes.
- **FHIR-Based Exchange at Scale:** Recent updates to TEFCA incorporate Fast Healthcare Interoperability Resources (FHIR) API-based exchange, intended to allow participants to leverage modern, standards-based APIs for scalable, nationwide data sharing.
- **Individual Access Services:** TEFCA envisions enabling individuals to access their health information through participating entities, supporting patient empowerment and compliance with federal access requirements.

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?

The data provided by HIEs is increasingly valuable and accurate, which should support whole-person care and improve outcomes. HIEs are intended to aggregate information from diverse sources, making it easier for providers to avoid redundant tests and for patients to stay informed and engaged in their own care. However, the quality and completeness of data can still vary depending on the region and the level of participation among local healthcare organizations.

b. What changes would you suggest?

CHI sees several opportunities to further enhance the impact of HIEs. Standardizing data formats and interoperability protocols should ensure that information flows smoothly and is easily usable across different systems, which would be assisted by actual enforcement of the information blocking rules and the development of pro-innovation guidance in a transparent and responsive manner. Investing in data normalization and analytics could transform raw data into actionable insights for both clinicians and patients. Expanding patient-facing tools should also empower patients to access and understand their health information directly.

c. What is the ongoing role of HIEs amidst other entities facilitating data exchange and broader frameworks for data exchange (for example, vendor health information networks, TEFCA, private exchange networks, etc.)?

Even as new frameworks for data exchange emerge, such as vendor health information networks, TEFCA, and private exchange networks, HIEs continue to play a vital, complementary role. They act as community-focused hubs, offering localized expertise and supporting public health initiatives while integrating with broader national networks. As the healthcare data landscape evolves, HIEs are well-positioned to ensure that data exchange remains secure, patient-centered, and responsive to the unique needs of local communities.

PC-12. What are the most valuable operational health data use cases for patients and caregivers that, if addressed, would create more efficient care navigation or eliminate barriers to competition among providers or both?

a. Examples may include the following:
   (1) Binding cost estimates for pre-defined periods.
   (2) Viewing provider schedule availability.
   (3) Using third-party apps for appointment management.
   (4) Accessing patient-facing quality metrics.
   (5) Finding the right provider for specific healthcare needs.
b. What use cases are possible today?
c. What should be possible in the near future?
d. What would be very valuable but may be very hard to achieve?

Health data is rapidly transforming the patient and caregiver experience, with operational use cases that promise to make care navigation more efficient and foster greater competition among providers. Today, patients can already benefit from digital tools that allow them to view provider schedules, manage appointments through third-party apps, and, where available, access quality metrics and compare providers for specific healthcare needs. These tools are increasingly integrated into patient portals and mobile apps, connecting patients to care teams and streamlining the process of finding and booking care. Today, many of these use cases are possible, especially in advanced health systems and regions with robust digital infrastructure. Patients can

often use apps to schedule appointments, view some quality information, and even receive digital cost estimates for certain procedures.

The potential of health data is being held back by continued unlawful information blocking practices. In the most immediate, the Department of Health and Human Services should take steps to end information blocking practices that are actively harming patients, with a focus on health IT developers who view information blocking as a competitive advantage. While we appreciate HHS's efforts so far, existing information blocking rules are often ignored due to weak enforcement. Some entities offer ineffective "compliant" solutions or openly disregard the rules. To truly overcome barriers to health information exchange, the Administration must enforce these rules meaningfully, promptly address complaints, publish findings, and take action. Enforcement should be predictable and proportionate, ensuring real progress without undue burden.

3. Information Blocking and Digital Identity

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?

CMS has a unique opportunity to empower patients and caregivers by making it easier for them to report instances of information blocking through the ASTP/ONC Information Blocking Portal. By launching public awareness campaigns, CMS can ensure that patients and caregivers are well-informed about their right to access health information and the steps they can take if they encounter barriers. These campaigns might include digital outreach, printed materials in healthcare settings, and targeted messaging through Medicare communications.

In addition, CMS can work directly with healthcare providers, encouraging them to inform patients about the complaint process whenever access to information is denied or during care transitions. Integrating this information into discharge paperwork or patient portals ensures that patients receive timely guidance when it matters most.

To further lower barriers, CMS can simplify the reporting process, making it user-friendly, accessible in multiple languages, and available on mobile devices. Step-by-step guides and video tutorials can help patients and caregivers navigate the process with confidence. By partnering with patient advocacy organizations and caregiver networks, CMS can extend its reach, ensuring that more individuals have the support they need to file complaints when necessary.

As more patients and caregivers report information blocking, CMS and ONC will gain valuable insights into the recurring challenges and systemic barriers that hinder data exchange. This increased visibility enables targeted policy interventions and technical improvements, ultimately fostering a culture of transparency and data sharing across the healthcare system. The prospect of enforcement actions and disincentives for providers who engage in information blocking further motivates compliance, leading to more complete, accurate, and accessible health records.

Increased reporting not only enhances the quality of health information but also strengthens care coordination and patient outcomes. By actively encouraging and supporting the submission of

information blocking complaints, CMS can accelerate the transition to a truly interoperable health system, one where patients and caregivers are empowered, and data flows seamlessly to support better care for all.

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?

Patients and caregivers face several barriers to adopting digital identity credentials. Many are unfamiliar with the technology or lack digital literacy, particularly among older adults and those with limited experience using online tools. The enrollment process for digital identity solutions can be perceived as complex or intimidating, especially if it involves multiple steps, document uploads, or multifactor authentication. Concerns about privacy, data security, and the potential misuse of sensitive information also deter some users. Additionally, caregivers may encounter difficulties with delegated access, as current systems often lack clear mechanisms for granting appropriate permissions to family members or proxies.

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

Widespread adoption of digital identity credentials would offer significant advantages. Patients and caregivers could enjoy streamlined, secure access to health information across multiple platforms without needing to remember multiple usernames and passwords. Enhanced security measures, such as multifactor authentication, would better protect sensitive health data from unauthorized access and cyber threats. For caregivers, robust digital identity solutions could enable easier, more secure management of delegated access, ensuring that only authorized individuals can view or manage patient records. Overall, this would support more seamless care coordination, reduce administrative burdens, and empower patients to take a more active role in their healthcare.

c. What are the potential downsides?

Despite the benefits, there are potential downsides. Some patients may find the enrollment and authentication processes cumbersome or inaccessible, particularly those with limited digital skills or access to technology. There is also a risk that reliance on digital identity could inadvertently exclude vulnerable populations who are less able to obtain or use these credentials. Additionally, while advanced authentication methods improve security, they may introduce new risks, such as the compromise of biometric data, which cannot be reset like a password if breached.

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

Promoting the use of credentialing service providers (CSPs) would centralize and standardize the authentication process, making it easier for patients and caregivers to access health information from various sources using a single, secure digital identity. This would reduce friction, eliminate the need for multiple logins, and support interoperability across healthcare systems, apps, and provider portals. Improved access would facilitate better care coordination, timely sharing of information, and more informed decision-making by both patients and their caregivers.

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

CMS and payers can set standards for digital identity, incentivize adoption through policy and reimbursement, and conduct outreach to educate patients about the benefits and processes for obtaining credentials. Providers cab integrate digital identity solutions into their workflows, inform patients about their options, and support patients and caregivers through the enrollment process. App developers can work to ensure their applications accept standardized digital credentials and design user-friendly interfaces that accommodate users with varying levels of digital literacy.

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

CMS can play a pivotal role by launching public awareness campaigns, providing clear and accessible educational resources, and simplifying the process for obtaining digital credentials. Collaborating with community organizations, healthcare providers, and advocacy groups can help reach underserved populations. CMS can also encourage providers to inform patients about digital identity options during care interactions and offer technical support to assist with enrollment.

Providers

1. Digital Health Gaps

PR-1. What can CMS and its partners do to encourage providers, including those in rural areas, to leverage approved (see description in PC-5) digital health products for their patients?

a. **What are the current obstacles?**
b. **What information should providers share with patients when using digital products in the provision of their care?**
c. **What responsibilities do providers have when recommending use of a digital product by a patient?**

CMS and its partners can encourage providers, especially those in rural areas, to leverage approved digital health products by implementing a combination of financial incentives, streamlined coverage and reimbursement policies, technical support, and education.

First, CMS can update and modernize its payment and coverage policies to explicitly support the adoption of digital health technologies, making it easier for providers to receive reimbursement either directly for the technology or as part of bundled payments for care. This includes aligning incentives in both fee-for-service and value-based care models and encouraging Medicare Advantage plans to use their flexibility to expand access to digital health tools.

Second, financial incentives can be offered to providers who adopt and meaningfully use approved digital health products, with a particular focus on supporting practices in rural and underserved areas. CMS could also incentivize providers to submit outcome metrics related to digital health product use, helping to build the evidence base for these tools while rewarding early adopters.

Third, CMS should provide technical assistance, training, and outreach tailored to the unique needs of rural providers, addressing barriers such as limited broadband, workforce shortages, and lack of IT infrastructure. Partnerships with local organizations and health systems can further support adoption and integration.

Finally, clear beneficiary and provider communications, as well as streamlined regulatory processes, will help build trust and make it easier for providers to navigate the evolving digital health landscape.

By combining strategies like modernized reimbursement, targeted incentives, technical support, and robust communication, CMS can help ensure that providers across all settings, including rural areas, are equipped and motivated to leverage digital health products for their patients.

PR-2. What are obstacles that prevent development, deployment, or effective utilization of the most useful and innovative applications for physician workflows, such as quality measurement reporting, clinical documentation, and billing tasks? How could these obstacles be mitigated?

Obstacles that hinder the development, deployment, and effective use of innovative applications for physician workflows, such as quality measurement, clinical documentation, and billing, include high financial costs, workflow disruption, lack of interoperability, insufficient technical support, and limited digital skills among staff and physicians. Upfront and ongoing expenses, uncertainty about return on investment, and inadequate reimbursement are major deterrents, especially for smaller practices. Many systems are not well integrated with existing workflows, leading to increased workload, productivity loss, and resistance from clinicians who find the tools cumbersome or poorly matched to their needs.

Technical barriers such as unreliable systems, lack of interoperability, and insufficient vendor support further complicate adoption and effective use. Additionally, a lack of ongoing training and support, as well as concerns about data privacy and security, contribute to reluctance among providers.

To mitigate these obstacles, strategies should include:

- Improving usability and usefulness of digital solutions through user-centered design and close collaboration with clinicians during development.
- Enhancing interoperability and integration with existing systems to streamline workflows and reduce redundant data entry.
- Providing ongoing training, technical support, and resources tailored to varying levels of digital literacy among staff.
- Offering better reimbursement models and financial incentives to offset costs and reward meaningful use of digital tools.
- Ensuring robust privacy and security protections to build trust among providers and patients.

Further, CHI has worked to proactively address health AI governance and policy issues based on consensus views that span the healthcare sector, from technology developers to providers to patients, and we urge for alignment with:

- The CHI community's Health AI Policy Principles (https://connectedhi.com/wp-content/uploads/2022/02/Policy-Principles-for-AI.pdf);
- CHI recommendations on advancing transparency for AI in the healthcare ecosystem (https://connectedhi.com/wp-content/uploads/2022/02/AdvancingTransparencyforArtificialIntelligenceintheHealthcareEcosystem.pdf);
- CHI's AI Roles and Interdependencies Framework (https://connectedhi.com/wp-content/uploads/2024/02/CHI-Health-AI-Roles.pdf); and
- CHI's recommendations to the Department on Government Efficiency on ways to use AI to improve healthcare governance efficiency (https://connectedhi.com/wp-content/uploads/2025/01/CHI-DOGE-Recommendations-30-Jan-2025.pdf).

PR-3. How important is it for healthcare delivery and interoperability in urban and rural areas that all data in an EHR system be accessible for exchange, regardless of storage format (for example, scanned documents, faxed records, lab results, free text notes, structured data fields)? Please address all of the following:

a. **Current challenges in accessing different data formats.**
b. **Impact on patient care quality.**
c. **Technical barriers to full data accessibility.**
d. **Cost or privacy implications of making all data formats interoperable.**
e. **Priority level compared to other interoperability needs.**

Ensuring that all data in an EHR system, regardless of storage format, is accessible for exchange is crucial for both urban and rural healthcare delivery and interoperability, but several challenges and trade-offs must be addressed:

- **Current challenges in accessing different data formats:** EHR systems often store information in a mix of structured fields, such as free text notes, scanned documents, faxes, and lab results, each using different formats and standards. This lack of standardization makes it difficult to extract and share comprehensive patient information across systems. Most healthcare organizations struggle to access and exchange data in non-standard formats, which can lead to incomplete patient records and hinder communication among providers.
- **Impact on patient care quality:** When providers cannot access all relevant patient data, such as operative reports, encounter notes, or test results, critical information may be missed, leading to medical errors, duplicate testing, and suboptimal care decisions. This is especially problematic when patients transition between care settings or providers, as incomplete data can directly impact safety and outcomes.
- **Technical barriers to full data accessibility:** Technical challenges include the use of proprietary or incompatible data formats, lack of adoption of interoperability standards (like HL7, FHIR), and difficulty extracting data from unstructured sources (such as scanned documents or free text). Integrating disparate systems and normalizing data for meaningful exchange requires significant technical investment and expertise.
- **Cost or privacy implications of making all data formats interoperable:** Transforming all data formats for interoperability can be expensive, requiring new software, staff training, and ongoing maintenance. Privacy and security concerns are heightened as more data becomes accessible and exchangeable, making compliance with regulations like HIPAA more complex and critical. There is also a risk of exposing sensitive data if robust security measures are not in place.
- **Priority level compared to other interoperability needs:** While making all data formats interoperable is highly important for comprehensive, high-quality care, it must be balanced with other priorities such as data security, patient privacy, and cost-effectiveness. Standardizing structured data fields and adopting open APIs (like FHIR) are often seen as foundational steps but expanding interoperability to include unstructured and legacy

formats is increasingly recognized as essential for closing information gaps and improving care, especially in resource-limited rural settings.

In summary, full accessibility of all EHR data formats is vital for optimal care and research, but requires overcoming significant technical, financial, and privacy challenges. Prioritizing interoperability standards and investing in technologies that can extract and normalize data from all formats will be key to advancing healthcare delivery across diverse settings.

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?

To allow patients' third-party digital products to seamlessly handle administrative tasks like auto-populating intake forms, viewing provider schedules, and managing appointments, improvements to both technical standards and policies are needed. Expanding the use of FHIR APIs beyond clinical data to include administrative information is a crucial step, as it would enable secure, real-time access for apps to interact with provider directories, appointment systems, and intake workflows.

Policies should require healthcare providers and EHR vendors to make these administrative data points available through open, standardized APIs, ensuring that third-party apps can integrate smoothly with existing systems. At the same time, robust consent and access controls must be implemented, allowing patients to securely authorize which apps can access their administrative information.

Clear alignment with federal interoperability and information blocking rules is also necessary, making it explicit that administrative data must be as accessible as clinical data. Developing official implementation guides and certification processes for administrative workflows would help standardize integration and ensure reliability.

Finally, ongoing collaboration with patients, providers, and app developers will be essential to refine these standards and policies, making sure they address real-world needs and enhance the patient experience. With these changes, patients and caregivers could benefit from more efficient, user-friendly digital tools to manage their healthcare interactions.

2. Data Exchange

PR-5. Which of the following FHIR APIs and capabilities do you already support or utilize in your provider organization's systems, directly or through an intermediary? For each, describe the transaction model, use case, whether you use individual queries or bulk transactions, and any constraints:

a. **Patient Access API.**
b. **Standardized API for Patient and Population Services.**
c. **Provider Directory API.**
d. **Provider Access API.**
e. **Payer-to-Payer API.**
f. **Prior Authorization API.**
g. **Bulk FHIR, Do you support Group ID-based access filtering for population-specific queries?**
h. **SMART on FHIR, Do you support both EHR-launched and standalone app access? What does the process for application deployment entail?**
i. **CDS Hooks (for clinical decision support integrations).**

Provider organizations have adopted or are adopting many FHIR APIs and capabilities, often directly or through intermediaries, with varying transaction models, use cases, and constraints:

- **Patient Access API:** Patient access to API is widely supported because APIs enable patients to access their health data via third-party apps using FHIR. The transaction model is typically individual queries (RESTful GET requests) for patient-specific data. Use cases include patient engagement and personal health management. Constraints include authentication, consent management, and sometimes limited data scope.
- **Standardized API for Patient and Population Services:** Supported in organizations using modern EHRs or cloud platforms, standardized API for patient and population services enables both individual patient queries and population-level (bulk) data access for analytics, quality measurement, and research. Transaction models include both individual and bulk queries (e.g., $export for bulk data). Some constraints involve data privacy, filtering, and sometimes performance limitations for large exports.
- **Provider Directory API:** Increased adoption, particularly as required for payer-provider interoperability allows systems and apps to retrieve up-to-date provider information (e.g., names, specialties, locations) via FHIR endpoints. Transaction model is typically individual queries, but bulk downloads are possible for directory synchronization. Use cases include care coordination and network management. Constraints include data freshness and completeness.
- **Provider Access API:** This emerging capability, often used via intermediaries or as part of payer-provider data exchange initiatives, enables providers to access patient data from payers or other providers. Transaction model is usually individual queries, with some support for batch operations. Use cases include care transitions and closing information gaps. Constraints include authentication, authorization, and varying implementation maturity.
- **Payer-to-Payer API:** Adoption is driven by CMS mandates for payers, but some provider organizations participate as intermediaries or endpoints. Payer-to-Payer API facilitates the transfer of patient data between payers, especially during transitions of coverage. Transaction model is typically bulk or batch data exchange. Constraints include data mapping, consent, and timing of data transfers.
- **Prior Authorization API:** Rapidly evolving with growing support due to regulatory focus on reducing provider burden Prior Authorization API enables electronic submission and tracking of prior authorization requests. Transaction model is transactional (individual

requests and responses). Use cases are streamlining administrative workflows and reducing delays. Constraints include payer-specific requirements and incomplete standardization.

- **Bulk FHIR (Group ID-based access filtering):** Supported in organizations with advanced data infrastructure or cloud-based FHIR servers, Bulk FHIR enables bulk export of data for defined patient populations using Group IDs. Used for research, quality reporting, and population health management. Constraints include data privacy, export performance, and patient consent management.
- **SMART on FHIR:** Widely supported in modern EHRs and cloud platforms. Both EHR-launched and standalone app access are available, using OAuth 2.0 for secure authorization. App deployment requires registration, security review, and sometimes organizational approval. Use cases include clinical decision support, patient-facing apps, and workflow tools.
- **CDS Hooks:** Adoption is growing for clinical decision support integrations. Allows EHRs to trigger external CDS services at specific workflow points. Transaction model is event-driven, with real-time calls to CDS services. Use cases include alerts, reminders, and care recommendations. Constraints include integration complexity and variability in EHR support.

PR-6. Is TEFCA currently helping to advance provider access to health information?

a. **Please provide specific examples.**
b. **What changes would you suggest?**
c. **What other options are available outside of TEFCA?**
d. **Are there redundant standards, protocols or channels or both that could be consolidated?**

TEFCA (Trusted Exchange Framework and Common Agreement) introduces several unique interoperability functions that set it apart from previous efforts to connect healthcare data nationwide, ultimately advancing provider access. However, TEFCA's implementation is not without its challenges. As we have noted on the record before, a proposed reliance on TEFCA could privilege licensed health care providers and exclude all other providers of healthcare services in creating a two tiered system where providers who are subject to federal privacy and security laws but are not licensed health care professionals as defined in TEFCA Standard Operating Procedures will have to undertake actions above and beyond those taken by licensed health care providers to ensure that their queries for patient health information for treatment are responded to and not blocked. The creation of such a dynamic is counter to the Cures Act requirement that "special effort" not be required.[2] In addition, by artificially siloing data from digital-first health care providers, the proposed rule severely hampers the access, exchange, and use of a growing subset of electronically accessible health information by the full ecosystem of providers in the interest of patients, as we'll discuss below regarding impact.

[2] 21st Century Cures section 4002, adding 42 USC 300jj-11(D)(iv)

Notably, TEFCA has the potential to facilitate access to comprehensive, standardized clinical information spanning various healthcare environments and regions for AI-driven applications. Despite this promise, availability of such data remains constrained. Typically, developers must collaborate with TEFCA-affiliated organizations, such as hospitals or health networks, and are restricted to using the information for specific functions, most often related to care delivery, billing, or administrative tasks. Broader applications, including the creation of AI algorithms, are generally not allowed under existing policies unless the data is anonymized or explicit patient consent is obtained. Future revisions to the framework could consider ways to responsibly broaden the range of acceptable uses.

The following will advance provider access to health information:

- **Nationwide Network-to-Network Connectivity:** TEFCA establishes a "network of networks" model, which envisions Qualified Health Information Networks (QHINs) connecting directly to each other, enabling seamless, secure exchange of electronic health information (EHI) across the country, regardless of the underlying technology or vendor.
- **Common Rules of the Road:** All participating Health Information Networks (HINs) and their members are bound by a single set of legal, technical, and operational requirements. This includes standardized authentication, authorization, privacy, and security policies, reducing fragmentation and simplifying participation.
- **Standardized Technical Framework:** The QHIN Technical Framework (QTF) specifies core interoperability functions such as certificate policy, secure channels, mutual authentication, user authentication, authorization, patient identity resolution, record location, directory services, privacy preferences, auditing, and error handling. These standards enable advanced functions like broadcast queries, targeted queries, and message delivery between QHINs.
- **Support for Multiple Exchange Purposes:** TEFCA is designed to support a broad range of use cases, including treatment, individual access, payment, healthcare operations, and public health, expanding beyond the limited purposes of earlier networks.
- **Governance and Oversight:** TEFCA provides a governance structure, including minimum required terms and conditions (MRTCs), additional required terms and conditions (ARTCs), and standard operating procedures (SOPs) to ensure compliance and resolve disputes.
- **FHIR-Based Exchange at Scale:** Recent updates to TEFCA incorporate Fast Healthcare Interoperability Resources (FHIR) API-based exchange, intended to allow participants to leverage modern, standards-based APIs for scalable, nationwide data sharing.
- **Individual Access Services:** TEFCA envisions enabling individuals to access their health information through participating entities, supporting patient empowerment and compliance with federal access requirements.

PR-7. What strategies can CMS implement to support providers in making high-quality, timely, and comprehensive healthcare data available for interoperability in the digital product ecosystem? How can the burden of increasing data availability and sharing be mitigated for providers? Are there ways that workflows or metrics that providers are already motivated to

optimize for that could be reused for, or combined with, efforts needed to support interoperability?

CMS can support providers in making high-quality, timely, and comprehensive healthcare data available for interoperability by implementing a combination of regulatory enforcement, technical support, and burden-reduction strategies.

Strategies to Support Providers:

- **Enforce Information Blocking Rules:** CMS requires providers to attest that they are not knowingly restricting interoperability or data sharing. Public reporting of non-compliant providers, as well as tying compliance to Medicare Conditions of Participation, creates strong incentives for timely and comprehensive data exchange.
- **Mandate and Standardize APIs:** CMS rules require payers and, increasingly, providers to adopt standardized APIs (such as FHIR) to facilitate seamless electronic data exchange with patients, payers, and other providers. These APIs support both clinical and administrative data sharing, reducing manual processes and enabling real-time access.
- **Streamline Administrative Processes:** By automating tasks like prior authorization and admission/discharge notifications through interoperable systems, CMS policies help reduce administrative burden while increasing data availability.
- **Provide Implementation Guides and Technical Resources:** CMS offers detailed implementation guides and standards to help providers adopt new technologies efficiently, minimizing confusion and technical barriers.
- **Align Interoperability with Existing Quality and Reporting Workflows:** Many providers are already motivated to optimize for quality measurement, value-based care, and regulatory reporting. CMS can further integrate interoperability requirements into these existing workflows and metrics, allowing providers to leverage current efforts (such as quality reporting or MIPS Promoting Interoperability attestations) to meet data sharing goals.

Mitigating Provider Burden:

- **Reduce Redundancy:** By aligning interoperability requirements with existing reporting and quality improvement activities, providers can avoid duplicative work and focus on a unified set of metrics.
- **Automate Data Exchange:** APIs and automated notifications reduce the need for manual data entry and faxing, freeing up provider time and resources.
- **Offer Technical Assistance:** Ongoing support and clear guidance on implementation can help providers, especially smaller or resource-limited practices, adopt and maintain compliant systems.

PR-8. What are ways CMS or partners can help with simplifying clinical quality data responsibilities of providers?

CMS and its partners can simplify clinical quality data responsibilities for providers by leveraging digital standards, aligning reporting requirements, and modernizing data collection and feedback processes (see below).

a. What would be the benefits and downsides of using Bulk FHIR data exports from EHRs to CMS to simplify clinical quality data submissions? Can CMS reduce the burden on providers by performing quality metrics calculations leveraging Bulk FHIR data exports?

Using Bulk FHIR data exports from EHRs to CMS offers significant benefits. Providers could automate the extraction and submission of large volumes of clinical data, reducing manual entry and the risk of errors. CMS could then perform quality metric calculations centrally, relieving providers of complex reporting tasks and enabling a "report once, use many times" approach. This would streamline compliance, lower administrative burden, and allow providers to focus more on patient care. However, challenges include ensuring data standardization, privacy, and the technical readiness of all EHR systems to support bulk exports. There may also be concerns about data completeness and the timeliness of feedback if CMS handles all calculations.

b. In what ways can the interoperability and quality reporting responsibilities of providers be consolidated so investments can be dually purposed?

Provider investments can be dually purposed by aligning interoperability and quality reporting requirements. This means integrating digital quality measurement into existing EHR workflows and leveraging the same data infrastructure for both clinical care and regulatory reporting. For example, digital quality measures (eCQMs) that use FHIR-based APIs can support both real-time clinical decision-making and automated quality submissions, reducing duplication of effort. CMS's move to harmonize measures across programs and prioritize digital, outcome-focused metrics further supports this consolidation.

c. Are there requirements CMS should consider for data registries to support digital quality measurement in a more efficient manner? Are there requirements CMS should consider for data registries that would support access to real-time quality data for healthcare providers to inform clinical care in addition to simplifying reporting processes?

CMS should require data registries to support FHIR-based digital quality measurement, ensuring data is standardized and interoperable across systems. Registries should also provide real-time or near-real-time access to quality data for providers, enabling rapid feedback and continuous quality improvement at the point of care. This includes integrating patient-reported outcomes and embedding feedback into EHR workflows, making quality data actionable for clinical care as well

as reporting. Additionally, registries should harmonize measures and support a unified submission process to further reduce burden and complexity.

3. Digital Identity

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?

CMS can encourage providers to accept digital identity credentials by establishing clear standards, providing technical and operational support, and aligning incentives to streamline patient access and reduce administrative burden.

CMS is already moving toward a federated, modern identity verification solution for Medicare, aiming to allow patients to verify their identity once and use that credential across multiple systems, including providers and payers. This approach would eliminate the need for patients to manage separate logins for each provider, improving user experience and reducing friction in accessing digital health services.

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?**

Providers will need help with technical integration, workflow redesign, and assurance that these credentials meet security and regulatory requirements. CMS can support this by:

- Issuing clear technical standards and certification requirements for digital identity solutions, ensuring compatibility with provider EHRs and patient portals.
- Offering implementation guides and best practices, as well as technical assistance, to ease the transition and address provider concerns about security, liability, and patient matching.
- Aligning incentives, such as tying adoption of standardized digital identity credentials to quality reporting, interoperability requirements, or reimbursement programs, to motivate provider uptake.
- Providing education and outreach to build trust and awareness among providers and patients.

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?**

CMS can balance patient privacy with convenience and access to digital health products by adopting a multi-faceted approach that prioritizes both data protection and user-friendly access.

CMS's recent initiatives emphasize developing secure, interoperable digital health infrastructure, such as modern identity verification solutions (e.g., Login.gov, CLEAR), allow patients to access their health information and digital services across multiple providers without needing separate logins for each relationship.

To achieve this balance, CMS should advance policies that require strong privacy and security standards for all digital tools, ensuring that patient data is only shared with explicit consent and is protected. At the same time, CMS should encourage the use of APIs and digital identity credentials to streamline access, reduce administrative burdens, and empower patients to manage and share their health information as needed.

By combining robust technical safeguards, clear consent processes, and simplified access mechanisms, CMS aims to make digital health products both safe and convenient, enabling patients to benefit from innovative services while maintaining control over their sensitive health data.

PR-10. Regarding digital identity credentials (for example, CLEAR, Login.gov, ID.me, other NIST 800-63-3 IAL2/AAL2 CSPs):

a. What are the challenges and benefits for providers?

Providers benefit from digital identity credentials through simplified credentialing, reduced administrative burden, and improved data security. Modern solutions allow clinicians to maintain a single, portable credential profile, streamlining onboarding, payer enrollment, and multi-facility practice while reducing redundant paperwork. Automated reminders and digital profiles also help manage expirations and compliance. However, challenges include technical integration with legacy systems, ensuring compliance with privacy regulations, managing access permissions, and overcoming resistance to change. Providers may need support with workflow redesign and staff training to fully realize these benefits.

b. How would requiring their use improve access to health information?

Mandating digital identity credentials enables patients and providers to access and share health data more efficiently and securely. Patients can use a single, verified credential across multiple organizations, reducing repetitive onboarding and minimizing errors. This approach supports seamless, patient-centric data exchange, improving care coordination and reducing delays in accessing records or services.

c. What are the potential downsides?

Potential downsides include the risk of excluding patients or providers who lack digital literacy or access to required technology. Implementation costs, integration complexity, and the need for robust support and training can also be barriers. There are privacy concerns if credentials are not managed with strong safeguards, and over-reliance on a single system could pose risks if compromised.

d. What impact would mandatory credentials have on a nationwide provider directory?

Digital identity credentials would improve the accuracy and reliability of a nationwide provider directory by ensuring that each provider is uniquely and verifiably identified. This would reduce duplicate or outdated entries, streamline updates, and facilitate secure data sharing across organizations.

e. How could digital identity implementation improve provider data flow?

Digital identity streamlines data flow by enabling secure, permissioned access to provider profiles, credentials, and clinical data across systems. Providers can more easily share and update information, reducing administrative lag and errors, and accelerating onboarding, credentialing, and care transitions.

f. Would combining FHIR addresses and identity improve data flow?

Yes, combining FHIR addresses with digital identity credentials would further enhance data flow by linking verified identities to standardized data exchange endpoints. This would support automated, secure, and accurate routing of clinical and administrative information, ultimately improving interoperability and reducing manual intervention.

PR-11. How could members of trust communities (for example, QHINs, participants and subparticipants in TEFCA, which requires Identity Assurance Level 2 (IAL2) via Credential Service Providers (CSPs)) better support the goals of reduced provider and patient burden while also enhancing identity management and security?

Members of trust communities, such as QHINs, participants, and subparticipants in TEFCA, can better support reduced provider and patient burden and enhance identity management and security by leveraging standardized, high-assurance digital identity protocols and streamlining access processes.

- **Reducing Burden Through Federated Identity:** By adopting Identity Assurance Level 2 (IAL2) digital identity credentials, trust communities enable patients and providers to verify their identity once, then use that credential across all participating organizations. This

eliminates the need for multiple logins and redundant identity proofing, significantly reducing administrative overhead for both patients and providers. For patients, this means easier, more consistent access to their health records regardless of where care was provided, while providers benefit from simplified onboarding, credentialing, and data sharing workflows.

- **Enhancing Security and Trust:** TEFCA's requirement for IAL2 identity proofing ensures that only verified individuals can access sensitive health information, reducing the risk of unauthorized access and fraud. Credential Service Providers (CSPs) approved under NIST 800-63-3 standards provide robust, auditable processes for identity verification, supporting both privacy and security. This high level of assurance builds trust across the network and among patients, providers, and payers.
- **Streamlining Data Exchange and Access:** With IAL2 credentials, QHINs and other participants can automate and standardize access to health data, supporting both document-based and FHIR-based exchanges. This enables real-time, secure data retrieval and sharing, improving care coordination and empowering patients to manage their health more effectively. The consistency of identity management across the ecosystem reduces errors and delays, further lowering burden.

  Notably, trust communities are subject to information blocking regulations, which means they are required to facilitate, not hinder, the access and exchange of EHI, including through robust and interoperable identity management systems. Enforcement of the information blocking rules is therefore needed to trust communities' support the goals of reduced provider and patient burden while also enhancing identity management and security.

4. Information Blocking

PR-12. Should ASTP/ONC consider removing or revising any of the information blocking exceptions or conditions within the exceptions (45 CFR part 171, subparts B through D) to further the access, exchange, and use of electronic health information (EHI) and to promote market competition?

No, ASTP/ONC need not remove or revise any of the information blocking exceptions or conditions within the exceptions (45 CFR part 171, subparts B through D) to further the access, exchange, and use of electronic health information (EHI) and to promote market competition.

The free flow of information and interoperability are therefore important and life-saving for patients. A truly interoperable healthcare system facilitates patient engagement across a range of modalities with open application programming interfaces (APIs) that allow the safe and secure introduction of patient-generated health data (PGHD) into electronic health records (EHRs). Data stored in standardized and structured formats with interoperability facilitated by APIs provides analytics as well as near real-time alerting capabilities. The efficacy of precision medicine, population health, and clinical decision support – all critical means for combatting chronic diseases – is dependent in large part on the availability of data.

We emphasize the linkage of ensuring interoperability to the Administration's priority for leveraging the tremendous potential of artificial intelligence (AI). Many AI use cases, ranging from solving administrative/backend efficiencies to supportive clinical decisions, have already begun to emerge as necessary to advancing the Quadruple Aim. Data exchange, use of standardized terminologies, and the normalization of data flows across the care continuum, are a must if AI is to positively transform the American healthcare system.

The 21st Century Cures Act prohibits providers, developers, health information exchanges (HIEs), and health information networks (HINs) from practices that are likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information (EHI) so that health information may be accessed, exchanged, and used without special effort through the use of application programming interfaces, including providing access to all data elements of a patient's EHR. Yet, Congress' goals in this law, passed in 2016, are far from realized. Although federal regulations have been fully in effect since 2022, patients and providers still face major barriers to interoperability and access to health information, often stemming from a subset of developers that elect to use tactics amounting to information blocking ((e.g., vendors who prohibit access to their FHIR API). These practices delay care coordination, undermine clinical decision-making, and stall innovation.

In the most immediate, the Administration should take steps to end information blocking practices that are actively harming patients, with a focus on health IT developers who view information blocking as a competitive advantage. While we appreciate the resources created thus far by HHS, it is critical that the Administration acknowledge that existing rules addressing information blocking are not consistently being followed due in large part to a lack of enforcement. While some are implicitly violating the rules (e.g., offering "compliant" information exchange mechanisms that do not work in practice while offering functional solutions in parallel for a fee), others are unapologetically ignoring the rules. We emphasize that enforcement should be meaningful so as not to be viewed as a mere cost of doing business.

If the Administration is going to accomplish its goal of overcoming barriers to the seamless exchange of health information across systems, it should first make immediate efforts to resolve information blocking complaints, publish its findings, and take action on them to ensure that a baseline of data exchange is occurring. Enforcement should contribute to a predictable environment while taking into consideration the severity of the alleged misconduct so as to avoid disproportionate impacts.

CHI is also concerned with ASTP's decision during the previous Administration to outsource significant policy decisions under the Trusted Exchange Framework and Common Agreement to third parties who did not engage in adequate consultations with impacted stakeholder communities before setting deeply impactful policies. Such decisions should be subject to notice and comment periods.

CHI further has concern with ASTP's decision to implement AI transparency reporting requirements for "predictive decision support intervention" AI in the electronic healthcare record space, which were adopted pursuant to the previous Administration's AI Executive Order. These reporting requirements overlap with existing requirements, and we urge for their withdrawal (or at minimum, their conversion into voluntary reporting measures).

PR-13. For any category of healthcare provider (as defined in 42 U.S.C. 300jj(3)), without a current information blocking disincentive established by CMS, what would be the most effective disincentive for that category of provider?

For healthcare providers as defined in 42 U.S.C. 300jj(3) who currently lack a CMS-established information blocking disincentive, the most effective disincentive would be to tie participation in key federal programs or eligibility for federal payments to compliance with information blocking rule compliance.

For provider categories not yet covered by these disincentives, such as those not enrolled in Medicare or not participating in these specific programs, the most effective disincentive would be to condition participation in any federally funded health program (including Medicaid, CHIP, or other grant-funded initiatives) on compliance with information blocking rules. Alternatively, CMS could publicly identify providers found to have engaged in information blocking, which could impact their reputation and patient trust.

PR-14. How can CMS encourage providers to submit information blocking complaints to ASTP/ONC's Information Blocking Portal? What would be the impact? Would it advance or negatively impact data exchange?

CMS can encourage providers to submit information blocking complaints to the ASTP/ONC Information Blocking Portal by accomplishing meaningful enforcement of the rules, increasing awareness of the portal, clarifying the complaint process, and emphasizing the importance of reporting for improving interoperability and patient care. Educational campaigns, integration of complaint submission links within provider-facing portals, and assurances of confidentiality and non-retaliation can further motivate providers to report instances of information blocking.

The impact of encouraging provider complaints would be positive for data exchange. Increased reporting would help regulators identify and address patterns of information blocking more effectively, leading to stronger enforcement and greater compliance with interoperability rules. This, in turn, would promote more open access, exchange, and use of electronic health information, benefiting both providers and patients. However, there may be concerns about increased administrative burden or fear of retaliation, so CMS should ensure that the complaint process is straightforward and supportive.

Payers

PA-1. What policy or technical limitations do you see in TEFCA? What changes would you suggest to address those limitations? To what degree do you expect these limitations to hinder participation in TEFCA?

Payers have voiced concerns about both policy and technical limitations within TEFCA that could significantly hinder their participation. From a policy standpoint, they find the benefits of TEFCA unclear, especially since its requirements are still evolving and do not yet fully address key payer needs such as prior authorization, risk adjustment, or quality reporting. The high infrastructure demands, requiring substantial investments in technology, security, and ongoing compliance, further add to their hesitation. Additionally, payers struggle with the challenge of aggregating and standardizing data from a variety of disparate EHR systems, making it difficult to validate and effectively use member data.

On the technical side, accurate patient matching remains a major barrier, as linking records across multiple systems is complex and often unreliable. Many payer organizations also rely on legacy platforms that are not easily compatible with TEFCA's technical requirements, making integration costly and complicated. Furthermore, while TEFCA is moving toward real-time data exchange, many payer workflows still depend on efficient bulk data access, a capability that is not yet fully supported.

To address these challenges, payers suggest that TEFCA should offer clearer guidance and expanded support for payer-specific workflows, invest in robust and non-proprietary patient matching solutions, and enhance its infrastructure to better support both real-time and bulk data exchange. Streamlining onboarding and compliance processes would also help reduce the resource burden for payers.

Until these limitations are resolved, many payers are likely to delay or avoid joining TEFCA, preferring private data exchange networks that offer more flexibility, lower costs, and faster implementation. As a result, these barriers could slow the progress toward nationwide interoperability and limit TEFCA's effectiveness within the payer community.

PA-2. How can CMS encourage payers to accelerate the implementation and utilization of APIs for patients, providers, and other payers, similar to the Blue Button 2.0 and Data at the Point of Care APIs released by CMS?

CMS can encourage payers to accelerate the implementation and utilization of APIs for patients, providers, and other payers by combining regulatory requirements, robust enforcement of information blocking rules, and practical support for API adoption.

Recent CMS regulations mandate that federally regulated payers, including Medicare Advantage, Medicaid, CHIP, and Qualified Health Plans, implement four key APIs: Patient Access, Provider Access, Payer-to-Payer, and Prior Authorization. These APIs, modeled after Blue Button 2.0 and Data at the Point of Care, must be in place by January 1, 2027, and are designed to streamline data exchange, improve care coordination, and enhance patient access to health information.

To ensure these APIs are not only implemented but actively used, CMS is tying compliance to participation in federal programs and leveraging the enforcement of information blocking rules. These rules prohibit payers from interfering with the access, exchange, or use of electronic health information and now carry significant penalties for non-compliance. By linking API utilization to information blocking enforcement, CMS creates strong incentives for payers to maintain open, functional data exchange channels.

In addition, CMS supports payers with recommended standards, implementation guides, and educational resources, lowering technical barriers and helping payers understand the operational benefits of APIs. Public reporting of compliance and performance metrics, as well as incentives for providers to use electronic prior authorization, further motivate adoption and utilization.

This multi-pronged approach, mandating APIs, enforcing information blocking rules, providing technical support, and aligning incentives, ensures payers accelerate their API strategies. The result is more timely, secure, and comprehensive health data exchange, advancing nationwide interoperability and improving outcomes for patients and providers alike.

PA-3. How can CMS encourage payers to accept digital identity credentials (for example, CLEAR, ID.me, Login.gov) from patients and their partners instead of proprietary logins?

CMS can encourage payers to accept digital identity credentials, such as CLEAR, ID.me, or Login.gov, by establishing clear standards, providing technical and operational support, and aligning incentives to streamline patient access and reduce administrative burden.

CMS is already moving toward a federated, modern identity verification solution for Medicare, aiming to allow patients to verify their identity once and use that credential across multiple systems, including providers and payers. This approach would eliminate the need for patients to manage separate logins for each provider, improving user experience and reducing friction in accessing digital health services.

PA-4. What would be the value to payers of a nationwide provider directory that included FHIR end points and used digital identity credentials?

A nationwide provider directory of FHIR endpoints would be a helpful resource for the healthcare sector writ large by greatly improving access to health information for patients, providers, and payers:

- **For Patients: The directory** simplifies connecting personal health apps to the right data sources. For example, a patient wanting to access their records from a state Medicaid agency or a hospital could easily find the correct FHIR server URL, enabling seamless, secure access to their health information.
- **For Providers:** Providers could quickly locate and connect to other organizations' FHIR endpoints for referrals, care coordination, and information exchange, reducing

administrative burden and minimizing errors caused by outdated or inaccurate contact information.
- **For Payers:** Payers benefit from streamlined data exchange with providers and other payers, enabling more efficient claims processing, care management, and compliance with interoperability regulations.

A centralized, validated directory would also reduce redundant effort and cost. Currently, providers must submit similar information to multiple payers and organizations, costing the industry billions annually and often resulting in outdated or inaccurate data. A national directory would serve as a single source of truth, supporting up-to-date, accurate, and validated information about endpoints and the organizations that use them.

While CHI takes no position on who should public such a directory, we believe that HHS (and the Assistant Secretary for Technology Policy) is well-positioned to support and oversee its creation and maintenance.

To maximize adoption and public benefit, basic access to the directory should be free or very low-cost for all. This approach encourages widespread use and supports the public good by enabling interoperability and reducing administrative burden.

PA-5. What are ways payers can help with simplifying clinical quality data responsibilities of providers?

Payers can play a significant role in simplifying clinical quality data responsibilities for providers by leveraging technology, streamlining data exchange, and consolidating reporting requirements.

a. **How interested are payers and providers in EHR technology advances that enable bulk extraction of clinical quality data from EHRs to payers to allow them to do the calculations instead of the provider-side technology?**

Both payers and providers have a strong interest in EHR technologies that enable bulk extraction of clinical quality data. These advances allow payers to directly access large volumes of structured and unstructured clinical data from EHRs, reducing the manual burden on providers to submit quality data or respond to repeated chart requests. When payers perform the quality metric calculations themselves, providers can focus more on patient care and less on administrative tasks, while payers benefit from more timely and comprehensive data for quality measurement and gap closure.

b. **In what ways can the interoperability and quality reporting responsibilities of providers to both CMS and other payers be consolidated so investments can be dually purposed? Are there technologies payers might leverage that would support access to**

real time quality data for healthcare providers to inform clinical care in addition to simplifying reporting processes?

Consolidation is possible by aligning interoperability and quality reporting requirements to use the same data infrastructure and workflows for both CMS and commercial payers. Technologies such as cloud-based clinical data exchange platforms, real-time bi-directional connectivity, and standardized APIs (like FHIR) can enable providers to submit data once, which can then be used for multiple reporting and care improvement purposes. Payers can also deploy dashboards and analytics tools that give providers access to real-time quality data, supporting both clinical decision-making and regulatory reporting. This dual-purpose investment streamlines operations and reduces duplicative work for providers.

PA-7. How can CMS encourage payers to submit information blocking complaints to ASTP/ONC's Information Blocking Portal? What would be the impact? Would it advance or negatively impact data exchange?

CMS can encourage providers to submit information blocking complaints to the ASTP/ONC Information Blocking Portal by accomplishing meaningful enforcement of the rules, increasing awareness of the portal, clarifying the complaint process, and emphasizing the importance of reporting for improving interoperability and patient care. Educational campaigns, integration of complaint submission links within provider-facing portals, and assurances of confidentiality and non-retaliation can further motivate providers to report instances of information blocking.

The impact of encouraging provider complaints would be positive for data exchange. Increased reporting would help regulators identify and address patterns of information blocking more effectively, leading to stronger enforcement and greater compliance with interoperability rules. This, in turn, would promote more open access, exchange, and use of electronic health information, benefiting both providers and patients. However, there may be concerns about increased administrative burden or fear of retaliation, so CMS should ensure that the complaint process is straightforward and supportive.

Technology Vendors, Data Providers, and Networks

This section is intended for all stakeholders to provide input on questions as they relate to use cases and workflows that involve technology vendors, data providers, and networks. While we certainly want technology vendors, data providers, and networks to answer questions in this section (and in other sections) from their point of view, we also invite all stakeholders to provide their viewpoints on the technology vendor, data provider, and network use cases as appropriate.

1. Ecosystem

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?

CMS should update its payment frameworks to encourage greater participation from those designing digital health technologies. As outlined in PR-1 and PA-5, current Medicare billing protocols often introduce avoidable paperwork and fail to reflect the substantial resources required to launch robust remote monitoring initiatives. Developers are mindful of prior setbacks, such as FDA-cleared tools that failed commercially due to limited adoption, when evaluating whether to enter the market. Insufficient uptake, frequently linked to reimbursement obstacles, can dampen enthusiasm for pursuing new digital solutions. To address this, CMS ought to remove location-based payment reductions that disadvantage providers in rural or lower-cost regions, ensure compensation rates are sufficient, and streamline billing processes that add complexity without tangible benefit.

Additionally, CMS should work toward establishing straightforward and reliable payment routes for high-impact digital health offerings. Many such innovations do not align with existing benefit classifications, making it unclear if or how they will be reimbursed. This ambiguity discourages investment and slows progress. One possible remedy is for CMS to create a digital health "sandbox" initiative, enabling early, informal collaboration between the agency and product creators. This would clarify expectations around coverage and evidence requirements. Drawing on CMS's prior experience with sandbox approaches in data sharing and interoperability, this model could provide a balanced yet adaptable structure to speed up the introduction of safe, effective digital health solutions for Medicare recipients.

Building on leaps forward made during President Trump's previous Administration, CMS has incredible opportunity to leverage the immense value of health innovations that improve healthcare outcomes and secure significant cost savings, including telehealth, remote patient monitoring, and AI:

> *Software as a Medical Device (SaMD) as a Direct Practice Expense:* We are encouraged that CMS recognizes that its existing practice expense (PE) methodology creates significant barriers to the uptake of digital health innovations through the classification of most SaMD as indirect practice expenses. However, CMS efforts to address this outdated and anti-innovation policy have stagnated, particularly during the previous administration.

While the existing PE methodology is meant to account for a physician practice's costs, both direct and indirect, the ongoing choice of CMS to categorize SaMD as an indirect practice expense discourages the uptake and use of SaMD, remains one of the largest barriers to meaningful Medicare payment reforms, and is long overdue for a change. CMS' indirect methodology leverages cost bases and uses physician work relative value units (RVUs) but does not account for other factors like device maintenance.

While CMS began considering SaMD an indirect cost in 2019,[3] CMS has more recently indicated an interest in revising its approach to SaMD. CMS has been cross-walking payment rates for SaMD-inclusive codes to what CMS would have paid if the SaMD product had been included as a direct input. CMS has an obligation to steward Medicare beneficiary access to leading SaMD solutions and should seize this opportunity to advance meaningful PE methodology reform. We ask CMS to make these valuable SaMDs more accessible to Medicare beneficiaries by evolving its PE methodology to reflect the value that software provides by incorporating the value of software into Current Procedural Terminology® (CPT) codes to address PE and/or work intensity for RVUs. Specifically, the value of services delivered by a physician to interpret or act on new digital health technology information should be included in work RVUs, and the value of the software used to address improvements and efficiency in patient care should be factored into practice expense RVUs.

As CMS allows for SaMD reimbursement as direct supply inputs, CMS should obtain the most accurate estimate of the per-service cost of the input as possible, particularly by relying on invoices. CMS' equipment amortization formula should only apply in the case of locally installed computer programs with an upfront payment where a useful life can be estimated and where that SaMD is only used in one service at one time.

CMS should also bring eligible digital health innovations into Medicare beneficiaries' care continuum by clarifying whether digital medical devices, such as SaMD, are included in existing benefit categories.

Consistent with CMS' clear authority and its obligation to improve Medicare beneficiary outcomes, we call on CMS (1) to act in its Calendar Year 2026 Physician Fee Schedule rulemaking to effect overdue changes to its PE methodology to accurately categorize and support the use of SaMD in Medicare; and (2) to then launch a standalone consultation to inform broader reforms to its PE methodology. We appreciate your attention to this important issue and look forward to working with you to broaden beneficiary access to SaMD.

Telehealth: In key Medicare payment rules (e.g., the Medicare Physician Fee Schedule) CMS has enabled the expanded use of telehealth, which is restricted to live voice/video calls in Medicare due to statutory restrictions. The previous Administration insisted on a read of the Social Security Act (SSA) that imposes outdated constraints that long ago

[3] *Medicare Program; Revisions to Payment Policies Under the Physician Fee Schedule and Other Revisions to Part B for CY 2019; et al*, 83 Fed. Reg. 59452, 59557 (Nov. 23, 2018).

ceased to have public benefit on where and to whom these services are made available. CHI requests that CMS revisit its read of the SSA to appropriately and permanently avoid the application of SSA Section 1834(m) restrictions on telehealth services, as well as asynchronous remote monitoring and other digital modalities.

Remote Monitoring: In the first Trump Administration, CMS enabled the use of remote physiologic monitoring (RPM) and remote therapeutic monitoring (RTM) services for both acute and chronic conditions in Medicare Part B, representing a monumental step forward in advancing the use of digital health tools in the care of America's most vulnerable populations. CMS' payments for RPM should be increased to provide much-needed support for this critical modality that is vital in preventing and treating the system's most expensive chronic conditions. CMS should step forward in removing outdated barriers to innovation and use of RPM and RTM through such steps as waiving co-pay requirements for these services and providing guidance on remaining questions plaguing the RPM and RTM tech developer and provider communities to support its wider use, which is already demonstrated to improve outcomes while reducing Medicare costs.

Artificial Intelligence: While your Administration took significant steps to support AI innovation in healthcare, the Biden-Harris Administration left many opportunities on the table, in some cases taking steps that have inhibited progress for health AI across prevention, treatment, or administrative contexts. We call on CMS to take much needed steps to recognize the value of countless AI tools (over 500 of which have already been approved by the FDA) to improve Medicare beneficiaries' experience and care,

Diabetes Prevention: Another area overdue for action by CMS in its Physician Fee Schedule is diabetes prevention. While there is a significant and growing body of empirical evidence showing the benefits of digital health technology for diabetes prevention and treatment, this condition imposes a significant burden on CMS' Medicare program and its beneficiaries, totaling hundreds of billions of dollars each year. However, diabetes care is well-suited to digital medicine innovations because it requires interpretation of many kinds of data that can be captured through automation and biosensors. CMS can address the burden diabetes places on the Medicare program by:

- Finally including virtual diabetes prevention program providers who are CDC-recognized as part of the Medicare Diabetes Prevention Program (MDPP) under section 1115A(c) of the Social Security Act. CHI supports this proposed expansion, and the classification of the MDPP in Part B, as a timely and necessary step to address the diabetes crisis in the United States. CMS has already acknowledged the use of connected health tech products and services will be vital to the success of the MDPP.[4]
- Supporting virtual diabetes self-management training (DSMT), which would eliminate costly and time-consuming barriers to utilization of DSMT. CMS should

[4] 85 Fed. Reg. 50074 (Aug. 17, 2020).

also define certified diabetes educators (CDEs) as providers of DSMT. A 2014 report by the American Medical Association-convened Physician Consortium for Performance Improvement National Committee for Quality Assurance found an overwhelming majority of DSMT is carried out in primary care offices by non-"qualified diabetes educators."[5] CMS has the regulatory authority in the DSMT authorizing statute,[6] which states a certified DSMT provider is "a physician, *or other entity or individual designated by the Secretary"* [emphasis added] that provides DSMT and other Medicare services, to define a CDE. Recognizing CDEs as providers of DSMT care, including in telehealth, would help to address this gap in diabetes care.

Quality Payment Program (QPP): In the context of the Medicare Access and CHIP Reauthorization Act of 2015 (MACRA)[7] implementation, we encourage the Trump-Vance Administration to prioritize an outcome-based approach, like those identified by Congress in MACRA, as opposed to an approach dependent on quantitative metrics. An outcome-based approach can support the inclusion of digital health tools in providing patient care as part of the Quality Payment Program (QPP).

CMS is still chasing the ideal of a value-based U.S. healthcare system. Unfortunately, utilization of digital health tools in the Merit-based Inventive Payment System (MIPS) and in Alternative Payment Models (APMs) remains unrealized. MACRA's implementation has not even begun to approach realizing congressional goals for the widespread development and uptake of APMs due to significant vulnerabilities in the existing process (e.g., a complete lack of coordination between the Physician-Focused Payment Model Technical Advisory Committee and the Center for Medicare & Medicaid Innovation, neither of which produced successful physician-led models). As a result, APMs that encourage the responsible use of innovative digital health tools are severely lacking.

CHI strongly encourages the Trump-Vance Administration to undertake a new effort to identify regulatory changes needed at the federal level to advance value-based care in the American healthcare system by leveraging digital technologies, with a focus on eliminating healthcare disparities. Such an effort should also prioritize new ways to incent innovation by private payers to systemically advance value-based care. CHI commits to work with HHS and any impacted stakeholders to develop a consensus path forward that will bring the vision of value-based care to fruition.

CMS can make major progress in QPP towards this goal through:

- Reducing the reliance on CMS program participation and the use of Certified Electronic Health Record Technology (CEHRT) through the continued evolution of the Promoting Interoperability (PI) Program. The Health Information Technology for

[5] American Medical Association-convened Physician Consortium for Performance Improvement National Committee for Quality Assurance. Adult Diabetes: Performance Measures. January 2014.

[6] 42 U.S.C. 1395x(qq).

[7] Medicare Access and CHIP Reauthorization Act of 2015, Public Law No. 114-10, 129 Stat. 87 (2015).

Economic and Clinical Health (HITECH) Act incented physicians to purchase and use electronic health records (EHRs). Digitizing medical records has helped reduce issues associated with paper charts and records, including legibility, access, and loss. However, excessive regulation and overly prescriptive federal requirements have created unintended consequences. Program participants are now bound to use poorly functioning CEHRT products, built primarily to measure and report on CMS requirements, and are disincentivized from adopting truly useful technology. CMS should identify methods to reduce the overreliance on CEHRT in its programs and allow for physician and patient choice to drive the adoption and use of health IT products, such as by leveraging the value of connected health technology innovations that build on CEHRT.

- Permitting a professional to satisfy the demonstration of meaningful use of CEHRT and information exchange through attestation, which is allowed under existing law. HITECH permits reporting via "other means specified by the Secretary," granting the Secretary the authority to allow provider attestation across all EHR reporting programs. CMS should create broad categories of PI objectives allowing physicians to attest "yes/no" to the use of CEHRT itself to achieve those categories. CMS should reevaluate the need for numerator/denominator requirements in its EHR reporting programs.
- Developing, and publicly releasing, a comprehensive vision of a diverse array of connected health products and services, including telehealth, remote monitoring, and AI, playing an integral role in the success of APMs, and provide specific incentives and credits for the responsible use of these digital health tools.
- Using Medicaid waiver authority to permit states to include dual eligibles in their telehealth programs and establish programs for dual eligibles like Diabetes Prevention Programs, as age appropriate.
- Waiving Medicare's telehealth restrictions (under Social Security Act Sec. 1834(m)) for all shared savings programs and APMs, including payment bundles and medical home demonstrations.

Home Health Prospective Payment System (HHPPS): CMS has included remote monitoring expenses used by a Home Health Agency (HHA) to augment the care planning process as allowable administrative costs that are factored into the costs per visit. Such a change ensures that remote patient monitoring is utilized on a cost per visit basis when it is used by an HHA to augment the care planning process and will result in a more realistic HHA Medicare margin calculation. Remote monitoring will be helpful in: (1) augmenting HHA services in the patient's plan of care; (2) enabling HHAs to more rapidly identify changes in a patient's clinical condition and to monitor patient compliance with treatment plans (further enabling more effective and efficient review and appropriate alteration of plans of care); and (3) augmenting home health visits. However, CHI strongly urges CMS to align its definition of "remote patient monitoring" in the HHPPS with that captured in relevant CPT codes. While CMS correctly and proactively distinguishes between "remote monitoring" services and "telehealth" in this and other rulemakings, CHI suggests that CMS, in the HHPPS, contribute to a common definition of "remote patient monitoring" across its beneficiary programs (e.g., consistency with relevant CPT codes).

The HHPPS is also overdue for modernization to permit the use of digital health innovations that would benefit both providers and beneficiaries. CHI requests that CMS undertake a new effort, including a public consultation, to address ways the HHPPS can be modernized and improved. We commit to work with CMS and any other impacted stakeholders to develop and advance consensus policy changes.

Medicare Advantage (MA): CMS should provide MA plan sponsors with the discretion to make the determination that different digital health services are clinically appropriate, and to offer those services to beneficiaries as needed. CMS should make clear that those services that do not meet the definition of Medicare telehealth services (in other words, all services that are not live voice/video calls) do not face the onerous restrictions of Section 1834(m) of the Social Security Act. Currently, regulations provide that MA plans cover Part B benefits provided via electronic exchange as "additional telehealth benefits" (including RPM) and as a basic benefit as defined in § 422.101. We strongly encourage CMS to ensure MA plans' alignment with CMS' established approaches to Medicare fee-for-service telehealth services, including remote patient monitoring and other "remote communications technology" that CMS has expressly stated do not fall under 1834(m) and its restrictions. CMS should also fully leverage the potential of AI in accomplishing MA goals.

In addition, CMS should modify its MA/Part D and Accountable Care Organization risk adjustment policy to incorporate diagnoses from digital health-enabled remote encounters, including audio-only telehealth services where clinically appropriate.

Medicare Shared Savings Program: CMS should exercise its statutory authority under 42 U.S.C. 1395jjj(f) to waive Medicare Shared Savings Program payment and program requirements as appropriate to allow for one-sided and two-sided risk models under a waiver of telehealth restrictions. This would help providers that use APMs to reduce costs and meet statutory requirements. CMS recently exercised relevant waiver authority on several aspects of telehealth for two-sided risk models only. Doing so more broadly would further the success of APMs.

Center for Medicare and Medicaid Innovation (CMMI): Even CMMI's newest models do not adequately focus on exploring innovative technological healthcare delivery mechanisms. A 21st century healthcare system should embrace the array of new technologies available, such as RPM technologies and asynchronous store-and-forward methods, which enable the delivery of healthcare solutions beyond the four walls of a hospital room or doctor's office. The Trump-Vance Administration should prioritize a new CMMI path which embraces the use of new technologies in Medicare and Medicaid that will widely benefit beneficiaries.

CMMI should also take new steps to reduce the burdens for potential model applicants. CMMI should articulate consistent requirements that are applicable to all models being tested, rather than developing separate requirements for each. The burden for applicants and participants could be reduced through uniform processes, expectations, principles,

and rules that span models like population health and chronic conditions that are being tested. To align payers with the goals of the CMMI models and incent their participation, CMS should build upon the QPP to encourage the development of models that are based on existing structures and payment models and allow existing networks to apply as Advanced APMs to make these entities eligible for Medicare bonuses and programs like MIPS and the QPP. In exploring the benefits of telehealth as defined in 1834(m), CMS should use its established authority to waive the backward-facing and outdated restrictions. CMMI should also focus on exploring new and innovative remote monitoring technologies (which are not telehealth under 1834(m) and therefore do not face its geographic, originating site, etc., restrictions). We further urge CMMI to build upon the successes of the Veterans Health Administration in its use of connected health technologies.

CMMI should also recognize and build upon the incredible successes of health systems such as the University of Mississippi Medical Center, the University of Virginia, and Boston Children's Hospital. In these locations (and some others), Medicaid programs have taken steps to support not only telehealth but, more importantly, remote monitoring innovations that bring patient-generated health data (PGHD) into the continuum of care based on demonstrated improvements to patient outcomes and significant cost savings. CMMI can and should play a crucial role in proliferating these successes.

CMS should also continue support beneficiary engagement in accountable care relationships and quickly address the pending expiration of CMMI's Accountable Care Organization (ACO) Realizing Equity, Access, and Community Health (REACH) model on December 31, 2026. Absent timely interventions, beneficiary care may be impacted as model participants will have insufficient time to plan for ongoing care coordination.

Durable Medical Equipment (DME): CMS should, under its existing authority, discard the arbitrary limitations it places on DME payments to support the responsible uptake and use of digital health technology innovations. CMS' approach today to DME either entirely excludes or insufficiently supports the use of software in medical equipment that is increasingly essential to cutting-edge care. CMS is long overdue to provide a pathway for coverage under DME for software as a medical device (SaMD) that is primarily utilized for a medical purpose even when there are other uses of the software or the product the software is in. For example, if a device is capable of acting as a pulse oximeter and heart rate monitor, then it should be eligible for coverage as DME even if the device has other non-medical capabilities. DME coverage of software should also extend to SaMD therapeutics cleared by the FDA. In addition, support for such software in DME should be unbundled, with needed updates to the software supported as DME supplies when they are integral to the functioning of the underlying DME software.

CMS can take modest steps today to improve the DME program. For example, while CMS established that "therapeutic continuous glucose monitors (CGMs)" can be billed to CMS for both the DME component and an all-inclusive supply allowance, in 2018 local Medicare contractors issued a coverage determination that resulted in rejection of the supply allowance if a smart tablet or smartphone-compatible mobile medical app is used in conjunction with the CGM device and biosensors. This interpretation by Medicare

contractors was not dictated by law and resulted in a programmatic policy that ignores the many efficiencies of secure connected medical technologies that have the ability to ease the burdens on patients while reducing costs to Medicare in DME payments. CMS has the ability to change their course under existing authority and appears to have intervened to address the decisions of local Medicare contractors in this specific instance; however, due to the continued confusion created by Medicare contractors and CMS' policy correction regarding CGMs, CHI strongly urges CMS to ensure that the use of dual-use connected technology as DME is permitted widely through its DME rules.

DME enabled by internet connectivity and new, innovative features can and should be permitted to meet CMS' requirement for face-to-face encounters. Care providers can leverage connected health technology to obtain DME PGHD for continual evaluation and treatment of conditions. Such capabilities negate the need for an annual demonstration of medical necessity through their ongoing collection and transmission of PGHD. Therefore, CMS should eliminate this annual certification requirement when RPM can demonstrate medical necessity.

Part D: CHI generally supports CMS' work to provide clarity on Medicare Part D plan sponsor requirements but remains concerned that CMS is not enabling the maximum potential of digitally-enabled pharmacies that provide convenient and efficient home delivery that Americans across the country expect. CMS should take clear steps to support digitally-enabled pharmacies by avoiding applying the same requirements to each pharmacy type, as the previous Administration proposed, which will hold back digitally-driven efficiencies from countless beneficiaries without benefit to them.

The agency should further support adoption of digital forward technologies through modernizing Medicare Part D's convenient access standards to reflect the current state of pharmacy access. New policies should support beneficiary choice and convenience by removing the distance-based geographic constraints and enable plans to meet such standards through non-PBM-owned mail-order pharmacies.

In alignment with ASTP, CMS should advance policy that allows pharmacies to directly surface real-time pharmacy benefit information for Medicare Part D beneficiaries at the point of sale, supporting choice, convenience and affordability.

Absent Congressional action to address the issue, CMS should promulgate rulemaking for standard terms and conditions for pharmacies participating in Medicare Part D that does not disadvantage digital-forward pharmacies unaffiliated with a Pharmacy Benefit Manager (part of the *any willing provider* language).

CMS must also take immediate action to unlock the potential of AI for all Americans. AI, powered by streams of data and advanced algorithms, has incredible potential to improve healthcare, prevent hospitalizations, reduce complications, and improve patient engagement. CHI recognizes that, as healthcare AI innovations continue to be developed and enter today's regulatory processes, policymakers at the legislative and regulatory levels and industry must collaborate to reach AI's full potential, while prioritizing patient safety. CHI has worked to proactively address health AI governance and policy issues based on consensus views that span the healthcare sector, from

technology developers to providers to patients. With respect to its AI-related considerations, we urge CMS to align with several CHI policy and governance recommendations:

- CHI's *Health AI Policy Principles*, a comprehensive set of recommendations across key areas that should be addressed by any policymaker considering AI's use in healthcare (available at https://bit.ly/3m9ZBLv);
- CHI's *Advancing Transparency for Artificial Intelligence in the Healthcare Ecosystem*, comprehensive recommendations on ways to increase the transparency of and trust in health AI tools, particularly for care teams and patients (https://bit.ly/3n36WO5); and
- CHI's *Health AI Roles and Interdependencies Framework*, which describes the health AI value chain, defining actors and describing roles for ensuring safety and efficacy as well as the interdependencies between these actors (https://connectedhi.com/wp-content/uploads/2024/02/CHI-Health-AI-Roles.pdf).

Finally, we also emphasize that it is crucial for coordination across HHS in achieving health data interoperability. ASTP/ONC and CMS should ensure that their rules and approaches are aligned to advance interoperability in a coordinated way and to avoid putting stakeholders into a position where they are forced to violate one rule (e.g., meet the requirements of the CMS interoperability rule but face ambiguities as to whether the requirements of an exception to ONC information blocking is being satisfied).

TD-2. Regarding CMS Data, to stimulate developer interest,

a. What additional data would be most valuable if made available through CMS APIs?

Expanding the data made available through CMS APIs could significantly enhance the utility of these platforms for patients, providers, payers, and developers. Based on current offerings and regulatory requirements, the following types of additional data would be especially valuable:

- **More Comprehensive Prior Authorization Data**: While CMS is moving toward including prior authorization information (excluding drugs) in Patient Access and Payer-to-Payer APIs, expanding this to include all prior authorizations (including drugs) and more granular status updates would improve transparency and care coordination.
- **Real-Time Claims and Encounter Data**: Current APIs often provide claims and encounter data with some lag (e.g., weekly or monthly updates) making real-time or near-real-time data available would enable more timely interventions and better decision-making for providers and care managers.
- **Provider Remittance and Cost-Sharing Information**: Existing APIs often exclude provider remittance and enrollee cost-sharing details from claims and encounter data. Including this information would help patients better understand their financial responsibilities and support more accurate cost estimations for providers and payers.

- **Expanded Provider Directory Details**: While provider directory APIs are required, adding richer data such as provider availability, appointment scheduling links, telehealth capabilities, and quality ratings would make these directories more actionable for patients and referring providers.
- **Historical Coverage and Plan Transition Data**: APIs could be enhanced to include a patient's historical plan enrollments, transitions between plans, and associated coverage periods. This would facilitate continuity of care and support more comprehensive risk adjustment and care management.
- **Social Determinants of Health (SDOH) Data**: Integrating SDOH data (e.g., housing, transportation, food security) would enable more holistic care planning and support value-based care initiatives. This type of data is increasingly recognized as critical for improving health outcomes but is not widely available via current CMS APIs.
- **Patient-Reported Outcomes and Experience Data**: Adding access to patient-reported outcomes, satisfaction surveys, and experience measures would provide a more complete picture of care quality and patient engagement.
- **Enhanced Prescription and Medication Data**: While some APIs provide drug coverage information, expanding to include real-time prescription fill data, adherence tracking, and formulary alternatives would support medication management and cost control1.
- **Quality and Performance Metrics**: Making provider- and plan-level quality performance data (e.g., HEDIS, STAR ratings) available via APIs would inform patient choice, support value-based contracting, and enable more robust analytics.
- **Interoperability with Non-CMS Data Sources**: Facilitating connections to state Medicaid data, commercial payer data, and public health registries through federated APIs would create a more complete and interoperable ecosystem

b. What data sources are most valuable alongside the data available through the Blue Button 2.0 API?

To maximize the value of the data available through the Blue Button 2.0 API, which provides Medicare beneficiaries with access to their claims history, coverage details, and demographic information, integrating additional data sources can create a more comprehensive picture of patient health and care needs.

The Blue Button 2.0 API primarily supplies claims data (including inpatient, outpatient, skilled nursing, hospice, home health, professional, durable medical equipment, and prescription drug events), patient demographics, and insurance coverage information, all formatted according to the HL7 FHIR standard. While this is a robust foundation, there are several complementary data sources that, when combined with Blue Button 2.0 data, offer significant added value:

- **Electronic Health Record (EHR) Data:** EHRs contain clinical notes, lab results, imaging, immunizations, allergies, and vital signs, elements not present in claims data. Integrating EHR data provides a more complete clinical context for each patient.

- **Pharmacy Benefit Manager (PBM) Data:** While Blue Button 2.0 includes Medicare Part D prescription claims, PBM data can add real-time medication fill status, adherence information, and details on non-Medicare prescriptions.
- **Social Determinants of Health (SDOH):** Data on housing, transportation, food security, and other social factors can help identify non-medical barriers to care, which are not captured in claims or coverage data.
- **Provider Directory APIs:** Access to up-to-date provider directories, including provider specialties, locations, and appointment availability, can help patients and care teams coordinate care more effectively.
- **Patient-Reported Outcomes:** Surveys and patient-entered data on symptoms, quality of life, or treatment satisfaction add a patient-centered perspective that claims data alone cannot provide.
- **Imaging and Lab Information Networks:** Direct access to radiology images, lab test results, and pathology reports can fill gaps left by claims-based summaries.
- **Other Payer Data:** For patients with supplemental, Medicaid, or commercial insurance, integrating data from other payers can provide a unified view of all healthcare encounters and costs.

By combining Blue Button 2.0's Medicare claims and coverage data with these additional sources, applications can deliver more actionable insights, support better care coordination, and empower patients with a fuller understanding of their health.

c. What obstacles prevent accessing these data sources today?

Accessing additional valuable data sources through CMS APIs is prevented in a number of ways:

- **Information Blocking:** The Administration should take steps to end information blocking practices that are actively harming patients, with a focus on health IT developers who view information blocking as a competitive advantage. While we appreciate the resources created thus far by HHS, it is critical that the Administration acknowledge that existing rules addressing information blocking are not consistently being followed due in large part to a lack of enforcement. While some are implicitly violating the rules (e.g., offering "compliant" information exchange mechanisms that do not work in practice while offering functional solutions in parallel for a fee), others are unapologetically ignoring the rules. We emphasize that enforcement should be meaningful so as not to be viewed as a mere cost of doing business. If the Administration is going to accomplish its goal of overcoming barriers to the seamless exchange of health information across systems, it should first make immediate efforts to resolve information blocking complaints, publish its findings, and take action on them to ensure that a baseline of data exchange is occurring. Enforcement should contribute to a predictable environment while taking into consideration the severity of the alleged misconduct so as to avoid disproportionate impacts.
- **API Rate Limiting and Request Throttling**: CMS APIs often impose strict rate limits, restricting the number of requests a user or application can make in a given timeframe to

prevent system overload and ensure equitable access. For example, some APIs allow only a certain number of concurrent calls or requests per second and exceeding these limits results in errors or temporary blocks.

- **Data Fetching and Pagination Limits**: APIs frequently cap the number of records returned per request, requiring users to implement pagination or batching to access larger datasets. This can complicate data retrieval, especially for large-scale analyses, and may result in incomplete data if not handled properly.
- **Access Control and Permissions**: Some datasets require specific permissions, API keys, or app tokens for access. Role-based access controls and licensing agreements may restrict who can access certain data, limiting the availability of sensitive or proprietary information.
- **Security and Abuse Prevention**: To mitigate risks such as data breaches and denial-of-service attacks, CMS and similar platforms enforce security measures that restrict open access and require authentication. These measures, while necessary, can slow down or limit legitimate data use.
- **System Load and Fairness Considerations**: Limitations are designed to manage backend system load and ensure fair distribution of resources among all users. These controls may be adjusted without notice, making sustained or automated data extraction more challenging.
- **Technical Complexity and Error Handling**: Users must implement sophisticated logic for retrying requests, handling errors, and managing pagination, which increases development complexity. Failure to comply with these technical requirements can result in incomplete data retrieval or API access being blocked.
- **Data Retention and Historical Limits**: Some APIs only provide data for a limited number of years, restricting access to historical datasets that could be valuable for longitudinal analysis.

d. What other APIs should CMS and ASTP/ONC consider including in program policies to unleash innovation and support patients and providers?

To unleash innovation and better support patients and providers, CMS and ASTP/ONC should consider including a broader set of APIs in program policies, building on the current foundation of interoperability rules. The most impactful additions would be:

- **Provider Access API:** This API enables providers to access patient data held by payers, supporting more informed clinical decision-making and care coordination. It is already required under recent CMS rules and should remain a priority for broad adoption.
- **Payer-to-Payer API:** This API facilitates the transfer of patient health information between payers when a patient changes insurance, ensuring continuity of care and reducing data silos. This API is also mandated in recent regulations and is critical for seamless transitions.

- **Prior Authorization API:** This API automates and streamlines the prior authorization process, reducing administrative burden and expediting patient access to necessary care. This is a key focus of the CMS Interoperability and Prior Authorization Final Rule.
- **Bulk Data Access API (Flat FHIR or "FHIR Bulk"):** This API enables the secure, large-scale extraction of patient data for population health, research, and analytics, supporting learning health systems and advanced analytics.
- **Patient Access API (Enhanced):** While already required, continued evolution of this API to support richer data types (such as clinical notes, imaging, and social determinants of health) will further empower patients.
- **Provider Directory API:** This API offers up-to-date information on provider networks, specialties, and availability, supporting care navigation and network adequacy assessments.
- **Coverage Requirements Discovery and Documentation APIs:** These APIs help providers determine coverage and documentation requirements at the point of care, reducing claim denials and administrative delays.
- **SMART on FHIR and OpenID Connect Integration:** This API standardizes secure authentication and authorization for third-party apps, ensuring that only authorized applications can access sensitive health data.
- **Da Vinci Project Implementation Guides:** Adoption of Da Vinci IGs such as PDex (for payer data exchange), Prior Authorization Support (PAS), and Coverage Requirements Discovery (CRD) will further standardize and streamline key use cases.

2. Digital Identity

TD-3. Regarding digital identity implementation:

a. What are the challenges and benefits?

Digital identity implementation can greatly enhance security, making it much harder for unauthorized users to access sensitive patient information, reducing the risk of fraud. It can also streamline administrative tasks, making it easier for patients to access their records and for providers to coordinate care, especially when patients move between different health systems. With stronger digital identity systems, patients can take more control of their own data, and healthcare organizations can more easily comply with regulations by tracking who accesses what information.

Challenges to widespread adoption include that healthcare organizations must navigate a maze of privacy laws and ensure that digital identity solutions are both secure and user-friendly. Integrating systems with older, legacy technology can be technically daunting, and not all patients have the digital literacy or resources to use them effectively. Further, it is challenging to make sure different systems can work together, so patient records don't become fragmented.

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?

Requiring digital identity credentials, such as those provided by CLEAR, Login.gov, ID.me, or other NIST 800-63-3 IAL2/AAL2 certified providers, would have a significant impact on both cybersecurity and data exchange in healthcare.

On the cybersecurity front, implementing strong digital identity solutions would dramatically reduce the risk of unauthorized access to sensitive patient data. These credentials enforce robust identity verification and multi-factor authentication, making it much harder for malicious actors to breach systems or impersonate users. With healthcare organizations facing escalating cyber threats, including data breaches and ransomware attacks, a solid digital identity framework is a critical defense, helping to prevent identity theft, financial fraud, and the exposure of protected health information. Additionally, digital identity tools enable features like single sign-on and detailed audit trails, improving visibility into who accesses what data and allowing organizations to quickly detect and respond to suspicious activity.

For data exchange, standardized digital identity credentials streamline secure access across different systems and organizations. This consistency supports interoperability, ensuring that only verified users can access or share health information. It also simplifies compliance with regulations like HIPAA by providing clear access controls and auditability. However, successful implementation requires integrating these credentials with existing healthcare IT systems and ensuring user adoption, which can be challenging in environments with legacy technology or varying levels of digital literacy.

c. What impact would mandatory use of the OpenID Connect identity protocol have?

OIDC would strengthen cybersecurity by providing a standardized, robust authentication layer built on OAuth 2.0, OIDC to ensure that only verified users, whether patients, clinicians, or administrators, can access sensitive health data. This reduces the risk of unauthorized access, stolen passwords, and identity fraud, all of which are critical concerns in healthcare. OIDC supports advanced authentication methods, including biometrics and multi-factor authentication, and enables organizations to centrally manage and audit user access, further enhancing security.

For data exchange, OIDC enables streamlined and secure single sign-on (SSO) across multiple healthcare applications and services, whether on web, mobile, or cloud platforms. This not only simplifies the user experience but also supports interoperability by standardizing identity verification across disparate systems. With OIDC, credentials and authorizations can be managed in a single, secure location, reducing administrative overhead and making it easier to enforce consistent access policies.

Additionally, OIDC facilitates user-centric consent and authorization management, allowing patients to control who accesses their data and under what circumstances. This is particularly valuable for complying with privacy regulations and supporting patient empowerment.

However, integrating OIDC with legacy healthcare systems can be challenging, as not all existing platforms are designed for modern authentication protocols. Overcoming these technical hurdles is essential for realizing the full benefits of OIDC.

3. Technical Standards and Certification

TD-4. How can CMS better encourage use of open, standards-based, publicly available APIs over proprietary APIs?

CMS can better encourage the use of open, standards-based, publicly available APIs over proprietary APIs by leveraging a combination of regulatory requirements, technical guidance, and incentives:

- **Mandating Standards in Regulation:** CMS already requires payers and providers to implement APIs that adhere to specific, open standards, such as HL7 FHIR, US Core Implementation Guides, and SMART on FHIR, for patient, provider, payer-to-payer, and prior authorization data exchange. By continuing to update regulations to require the latest approved versions of these standards, CMS ensures that open APIs remain the default for health data exchange.
- **Providing Clear Technical Guidance:** CMS publishes detailed implementation guides and references for required APIs, eliminating ambiguity and reducing the burden on organizations to develop custom or proprietary solutions. These guides specify not only the standards themselves, but also recommended best practices for security, interoperability, and usability.
- **Aligning Certification and Compliance:** By tying the use of open, standards-based APIs to ONC Health IT Certification and program participation (such as Meaningful Use or Promoting Interoperability), CMS creates strong incentives for vendors and providers to adopt open APIs rather than proprietary alternatives.
- **Monitoring and Public Reporting:** CMS now requires annual reporting on API usage, including metrics on adoption and user engagement. Public reporting of these metrics increases transparency and motivates organizations to prioritize open API adoption to demonstrate compliance and leadership in interoperability.
- **Supporting Version Advancement:** CMS allows for the adoption of updated standards and implementation guides as they become available and are approved by the National Coordinator, ensuring that the ecosystem can evolve and improve without reverting to proprietary approaches.
- **Fostering an Ecosystem of Interoperable Apps:** By requiring open APIs and supporting frameworks like SMART App Launch and OpenID Connect, CMS enables a marketplace where third-party apps can securely connect to any compliant system, reducing vendor lock-in and encouraging innovation.

The Role of Standard-Essential Patents in Healthcare: The integration of standardized technologies into healthcare devices has transformed patient care, enabling real-time data exchange, seamless interoperability, and improved outcomes. Technical standards such as Wi-Fi,

Bluetooth Low Energy (BLE), and data exchange frameworks like FHIR and HL7 are now foundational to modern healthcare systems. However, the widespread adoption of these standards introduces complex challenges, including the licensing of standard-essential patents (SEPs). SEPs are deemed "essential" to a standard and can create concentrated market power, disrupt competition, stifle innovation, and escalate costs for manufacturers and healthcare providers.

- **The Value of Technical Standards:** Technical standards (e.g., 5G and Wi-Fi) establish common protocols and specifications that allow manufacturers to create equipment and software that work seamlessly together. Standardization is particularly effective when an uniform solution offers greater benefits than rapidly evolving, non-compatible technologies. In situations where the cost of frequent upgrades is high, and the advantages of such upgrades are limited, a stable, standardized foundation tends to serve the market more effectively.[8] In such cases, the value of the technology is significantly enhanced by the positive network externalities created through standardization, on its own, it may have little standalone utility.[9] By agreeing on these shared specifications, companies can spread the cost of establishing the standard across an industry while mitigating the risk of it not being adopted and reducing redundant development efforts that would arise from parallel development of competing proprietary solutions.[10] Without standards, healthcare providers would face a fragmented landscape of incompatible devices and systems, undermining quality and efficiency. Standardization is orchestrated by standards-development organizations (SDOs), which bring together industry stakeholders to identify and solve technical challenges. The result is uniform interoperability and product compatibility, reducing redundant development and spreading the cost of innovation across the industry.
- **Standard-Essential Patents:** Participants in the standards development process volunteer to contribute their patents to the standard in order to enable its widespread use. For example, if a data exchange protocol is standardized, any patent reading on that protocol becomes essential for compliance. This confers significant market power to the SEP holder, as manufacturers that are locked into the standard must license the patent to produce compliant products. To prevent a SEP holder's ability to abuse their inherently dominant market position in the standard while ensuring proper compensation for their technology contribution, the SDO requires a commitment to license the technology on fair, reasonable, and non-discriminatory (FRAND) terms. In a balanced and competitive standard-setting system, manufacturers compete to differentiate their products within the standardized framework, driving advances in design, user experience, and cost efficiency. This dynamic fosters a healthier market ecosystem, balancing interoperability, consumer choice, and sustained innovation.

- **Key Technical Standards in Healthcare Technology and Medical Devices**

[8] *See* Knutt Blind, *Standards and Innovation: What Does the Research Say?*, ISO Research & Innovation Papers at 8 (Jan. 2022), https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100466.pdf

[9] *See id.* at 9.

[10] *See id.*

- Wireless Connectivity Standards: Wireless connectivity standards are critical in modern healthcare, enabling devices to capture, share, and analyze patient data in real time. Technologies such as Wi-Fi, BLE, and advanced cellular protocols (4G, LTE, 5G) underpin a vast array of medical devices and telehealth solutions.
    - Wi-Fi is used in hospital environments and enables real-time transmission of patient data with minimal latency. For example, Philips IntelliVue patient monitoring systems use Wi-Fi to send vital signs and alerts to central stations, allowing clinicians to respond promptly to changes in patient conditions. Baxter's Sigma Spectrum infusion pump logs medication dosages and usage data directly into hospital systems, reducing manual errors and streamlining workflows. Even consumer devices like the Withings Thermo smart thermometer use Wi-Fi to sync temperature readings to mobile apps, expanding the ecosystem of connected health tools.
    - BLE is designed for secure, low-power data transfer, making it ideal for wearable and near-patient devices. The Dexcom G6 continuous glucose monitoring (CGM) system uses BLE to send real-time glucose readings to a patient's smartphone, eliminating the need for frequent fingerstick tests. Masimo's MightySat pulse oximeter transmits blood oxygen saturation and pulse rate to mobile apps, allowing both patients and providers to monitor trends over time. Fitness trackers like Fitbit Charge also leverage BLE to sync health metrics, integrating daily activity into broader care plans.
    - Cellular-compliant devices extend connectivity beyond hospital walls, ensuring critical data flows regardless of patient location. Devices like the iRhythm Zio patch use cellular signals to securely transfer cardiac data for continuous electrocardiogram (ECG) analysis. Telehealth kits such as TytoCare rely on cellular connections for remote examinations, and GreatCall's Lively Mobile Plus system provides emergency response services via cellular coverage. These capabilities are vital for maintaining uninterrupted, high-quality care for patients on the move.
    - The importance of these standards is recognized at the national level. For instance, the UK National Health Service's Future Connectivity program supports the installation of wireless infrastructure in hospitals, care homes, and ambulances, with pilot projects integrating wireless capabilities into ambulance bays.

- Data Exchange Standards: The shift from paper-based records to electronic health records (EHRs) has revolutionized healthcare data management.[11] However, the true value of EHRs is realized only when data can be seamlessly shared across providers and systems in routine and emergency situations. Data

[11] *See* Office of the Nat'l Coordinator for Health Info. Tech., *What Are the Advantages of Electronic Health Records?*, HealthIT.gov, https://www.healthit.gov/faq/what-are-advantages-electronic-health-records (last visited Feb. 26, 2025).

exchange standards ensure that patient information is accessible, portable, and interoperable. This open, standardized approach is also critical for innovation, allowing new tools, such as remote patient monitoring devices or telehealth platforms, to integrate without creating information silos. Ultimately, the faster and more reliable the sharing of patient data, the better clinicians can respond, especially in urgent or emergency situations where immediate access to accurate information can save lives.

- Health Level Seven (HL7) and FHIR**:** HL7 International is the leading organization for interoperability standards in healthcare. HL7 and its Fast Healthcare Interoperability Resources (FHIR) framework enable the secure exchange, integration, sharing, and retrieval of protected health information (PHI). These standards are relied upon by the vast majority of healthcare organizations, facilitating the flow of information between labs, imaging centers, specialists, and primary care providers with 95 percent of U.S. healthcare institutions operating on the HL7 V2.x standard for information systems and its adoption across 35 more countries.[12] Standards like the HL7 V2 and its successors (e.g., HL7 V3 and FHIR) have enabled healthcare to be truly digitized and streamlined, opening up opportunities for more personalized patient care and higher chances of administering life-saving medical treatments. For instance, Epic Systems' EHR platform relies on HL7 messaging to share patient data with other healthcare systems, resulting in more comprehensive patient records.[13] Notably, Epic Systems and Oracle Health (Cerner) hold over 50 percent of the domestic EHR market share, and they both rely on the HL7 standards. Epic Systems makes up 37.7 percent of the market share in the United States, with its international presence growing in prominent jurisdictions.[14] Cerner follows closely behind Epic Systems with 21.7 percent of the U.S. EHR market share.[15]
- DICOM and Management Standards: Other notable standards in the healthcare industry include the Digital Imaging and Communications in Medicine (DICOM) standard and technology management standards. The DICOM standard governs the exchange of medical imaging data, ensuring that images and related information can be shared across different equipment and systems. Technology management standards such as ISO 14971 (risk management) and IEC 62304 (software lifecycle processes) ensure that medical devices and systems are developed, integrated, and maintained with patient safety as a top priority.

[12] HL7 Version 2 Product Suite, Health Level Seven International, https://www.hl7.org/implement/standards/product_brief.cfm?product_id=185 (last visited Feb. 25, 2025).

[13] Epic Systems' Interoperability Guide for Clinical Information: HL7v2, Epic Systems, https://open.epic.com/clinical/HL7v2 (last visited Feb. 25, 2025).

[14] Maggy Bobek Tieché, *Most Common Inpatient EHR Systems by Market Share*, Definitive Healthcare (Jan. 10, 2024), https://www.definitivehc.com/blog/most-common-inpatient-ehr-systems.

[15] *Id*.

    - Interoperability standards are essential for timely, informed decision-making and continuity of care. They also support innovation by allowing new tools and platforms to integrate without creating information silos. The faster and more reliably patient data can be shared, the better clinicians can respond – especially in emergencies where immediate access to accurate information can save lives.

- **SEP Licensing Concerns in Healthcare:** When a technology becomes essential to a standard, the patent holder gains significant leverage. All manufacturers wishing to comply with the standard must license the SEP, potentially leading to inflated royalties and increased costs. In healthcare, these costs can be passed on to providers and, ultimately, patients. Anticompetitive SEP licensing tactics can disrupt competition by creating barriers to entry for smaller manufacturers who may lack the resources to negotiate or litigate SEP licenses. This concentration of power can stifle innovation, particularly if SEP holders engage in hold-up practices by demanding excessive royalties or refusing to license on FRAND terms. However, the adoption of standards also drives downstream innovation. Companies compete to differentiate their products within the standardized framework, leading to advances in design, usability, and efficiency. The challenge is to balance the benefits of standardization with the risks of SEP licensing abuse. Escalating SEP-related costs can have a direct impact on healthcare delivery. Higher device costs may limit access to advanced technologies, particularly in resource-constrained settings. Delays in deploying new devices due to licensing disputes can also affect patient care.
- **Policy and Regulatory Responses:** To address the challenges posed by SEPs, policymakers and regulators have emphasized the importance of FRAND licensing terms. These principles are designed to ensure that SEP holders cannot exploit their market power to the detriment of competition and innovation. Programs like the UK NHS Future Connectivity initiative illustrate the role of government in supporting the deployment of standardized technologies. By investing in connectivity infrastructure and promoting interoperability, such initiatives help ensure that the benefits of standardization are realized across the healthcare system.
- **The Future of Standardization and SEPs in Healthcare:** The continued evolution of healthcare technology will depend on the development and adoption of new standards. The growth of the internet of things (IoT) in healthcare, the expansion of telehealth, and the integration of artificial intelligence will all require robust, interoperable frameworks. The challenge moving forward is to maintain the benefits of standardization, interoperability, efficiency, and innovation, while managing the risks associated with SEPs. This will require ongoing collaboration among industry stakeholders, SDOs, regulators, and policymakers.

The integration of technical standards in modern healthcare is critical to ensuring that patients receive efficient care. While the SEP licensing landscape can create challenges related to market power, competition, and costs, careful policy and regulatory oversight can help ensure that the benefits of standardization are realized without stifling innovation or limiting access. As healthcare technology continues to evolve, the balance between standardization and innovation will remain a critical focus for industry leaders, policymakers, and clinicians alike.

TD-5. How could a nationwide provider directory of FHIR endpoints improve access to health information for patients, providers, and payers? Who should publish such a directory, and should users bear a cost?

A nationwide provider directory of FHIR endpoints would be a helpful resource for the healthcare sector by greatly improving access to health information for patients, providers, and payers:

- **For Patients:** Simplifying connecting personal health apps to the right data sources would greatly benefit patients. For example, a patient wanting to access their records from a state Medicaid agency or a hospital could easily find the correct FHIR server URL, enabling seamless, secure access to their health information.
- **For Providers:** Providers could quickly locate and connect to other organizations' FHIR endpoints for referrals, care coordination, and information exchange, reducing administrative burden and minimizing errors caused by outdated or inaccurate contact information.
- **For Payers:** Payers benefit from streamlined data exchange with providers and other payers, enabling more efficient claims processing, care management, and compliance with interoperability regulations.

A centralized, validated directory would also reduce redundant effort and cost. Currently, providers must submit similar information to multiple payers and organizations, costing the industry billions annually and often resulting in outdated or inaccurate data. A national directory would serve as a single source of truth, supporting up-to-date, accurate, and validated information about endpoints and the organizations that use them.

While CHI takes no position on who should public such a directory, we believe that HHS (and the Assistant Secretary for Technology Policy) is well-positioned to support and oversee its creation and maintenance.

To maximize adoption and public benefit, basic access to the directory should be free or very low cost for all. This approach encourages widespread use and supports the public good by enabling interoperability and reducing administrative burdens.

TD-6. What unique interoperability functions does TEFCA perform?

TEFCA (Trusted Exchange Framework and Common Agreement) introduces several unique interoperability functions that set it apart from previous efforts to connect healthcare data nationwide:

- **Nationwide Network-to-Network Connectivity:** TEFCA establishes a "network of networks" model, which envisions Qualified Health Information Networks (QHINs) connecting directly to each other, enabling seamless, secure exchange of electronic health information (EHI) across the country, regardless of the underlying technology or vendor.
- **Common Rules of the Road:** All participating Health Information Networks (HINs) and their members are bound by a single set of legal, technical, and operational requirements. This includes standardized authentication, authorization, privacy, and security policies, reducing fragmentation and simplifying participation.

- **Standardized Technical Framework:** The QHIN Technical Framework (QTF) specifies core interoperability functions such as certificate policy, secure channels, mutual authentication, user authentication, authorization, patient identity resolution, record location, directory services, privacy preferences, auditing, and error handling. These standards enable advanced functions like broadcast queries, targeted queries, and message delivery between QHINs.
- **Support for Multiple Exchange Purposes:** TEFCA is designed to support a broad range of use cases, including treatment, individual access, payment, healthcare operations, and public health, expanding beyond the limited purposes of earlier networks.
- **Governance and Oversight:** TEFCA provides a governance structure, including minimum required terms and conditions (MRTCs), additional required terms and conditions (ARTCs), and standard operating procedures (SOPs) to ensure compliance and resolve disputes.
- **FHIR-Based Exchange at Scale:** Recent updates to TEFCA incorporate Fast Healthcare Interoperability Resources (FHIR) API-based exchange, intended to allow participants to leverage modern, standards-based APIs for scalable, nationwide data sharing.
- **Individual Access Services:** TEFCA envisions enabling individuals to access their health information through participating entities, supporting patient empowerment and compliance with federal access requirements.

Notably, TEFCA has the potential to facilitate access to comprehensive, standardized clinical information spanning various healthcare environments and regions for AI-driven applications. Despite this promise, the availability of such data remains constrained. Typically, developers must collaborate with TEFCA-affiliated organizations, such as hospitals or health networks, and are restricted to using the information for specific functions, most often related to care delivery, billing, or administrative tasks. Broader applications, including the creation of AI algorithms, are generally not allowed under existing policies unless the data is anonymized or explicit patient consent is obtained. Future revisions to the framework could consider ways to responsibly broaden the range of acceptable uses.

TEFCA's implementation is not without its challenges, however. As we have noted on the record before, a proposed reliance on TEFCA could privilege licensed health care providers and exclude all other providers of healthcare services in creating a two tiered system where providers who are subject to federal privacy and security laws but are not licensed health care professionals as defined in TEFCA Standard Operating Procedures will have to undertake actions above and beyond those taken by licensed health care providers to ensure that their queries for patient health information for treatment are responded to and not blocked. The creation of such a dynamic is counter to the Cures Act requirement that "special effort" not be required.[16] In addition, by artificially siloing data from digital-first health care providers, the proposed rule severely hampers the access, exchange, and use of a growing subset of electronically accessible health information by the full ecosystem of providers in the interest of patients, as we'll discuss below regarding impact.

[16] 21st Century Cures section 4002, adding 42 USC 300jj-11(D)(iv)

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

The USCDI is central to enhanced interoperability of healthcare data by specifying a common set of data classes required for exchange and identifying a predictable, transparent, and collaborative process. We appreciate ONC's work to update the USCDI and its establishment of a process and structure to update and expand the USDCI as appropriate.

CHI supports the USCDI's proposed Version 5's Data Classes, which build on the data classes referenced by the 2015 Edition Common Clinical Data Set (CCDS) definition and includes Clinical Notes and Provenance. CHI further supports USCDI expansion, consistent with technology and competitive neutrality principles. CHI notes its support for the expansion of the USCDI to include social determinants of health (SDOH) with scaled security and privacy risk management practices that recognize the sensitivity of SDOH data that may be shared or disclosed. This includes incorporating SDOH data that considers social and environmental factors of patients' lives outside of the health care system in the USCDI with adequate safeguards, which requires ONC to coordinate with the HHS' Office for Civil Rights, standards development organizations, and other impacted stakeholders, which we support and encourage.

CHI reiterates our request that ONC clarify the role of testing and/or certification in the success of the Trusted Exchange Framework and Common Agreement (TEFCA) and in the establishment and development of USCDI. ONC has previously noted that once the final TEFCA is published, Qualified Health Information Networks (HINs) and their participants will be required to update their technology to support all the data classes included in USCDI in accordance with the requirements in the final TEFCA.

TD-8. What are the most effective certification criteria and standards under the ONC Health IT Certification Program?

The use of health IT past CEHRT offers the ability to improve care and keep patients safe. We urge that CMS move away from its reliance on CEHRT (through, for example, permitting health IT that builds on top of CEHRT) in order to provide increased competition in the marketplace as well as greater flexibility and choice for providers and patients. CHI notes its support of 2015 CEHRT requirements in 2019, but we reiterate our concern with, and lack of confidence in, any presumption that the 2015 ONC CEHRT standards will facilitate seamless interoperability.

The ONC Health IT Certification Program is most effective when it focuses on criteria and standards that drive true interoperability, data quality, and patient safety. Recent updates have made the United States Core Data for Interoperability (USCDI v3) the baseline, ensuring that all certified systems capture a broader, more standardized set of patient data, including social determinants of health and other key factors. Open, standards-based APIs like FHIR are now required, making it easier for patients and providers to securely access and share health information. Automated electronic case reporting to public health agencies is also mandated, which supports faster and more accurate disease surveillance. The program now addresses the

transparency and safety of AI-powered decision support tools, requiring clear documentation and risk management. Ongoing compliance is enforced through regular updates and strict privacy and security requirements, ensuring that certified systems remain secure and up to date.

TD-9. Regarding certification of health IT:

a. What are the benefits of redefining certification to prioritize API-enabled capabilities over software functionality?

Redefining health IT certification to prioritize API-enabled capabilities rather than just software functionality could offer several key benefits to healthcare. By focusing on open, standards-based APIs, certification ensures that health information can be accessed, exchanged, and used seamlessly across different systems, regardless of vendor. This approach directly advances interoperability, allowing patients, providers, and payers to securely share and retrieve comprehensive health data without special effort or proprietary barriers.

API-first certification should also support competition by enabling new applications and services to integrate with certified systems more easily, fostering a dynamic health IT ecosystem. It helps prevent information blocking, ensuring that patients can access their complete health records at no cost, and that data flows freely to support care coordination, public health reporting, and patient engagement.

Additionally, API-focused standards enhance security, privacy, and auditability by requiring robust authentication, authorization, and transparent documentation. This shift aligns health IT with national priorities for interoperability and patient-centered care, making certified systems more adaptable, future-proof, and responsive to evolving healthcare needs.

b. What would be the drawbacks?

Developing and maintaining secure, standards-based APIs can be costly and complex, especially for smaller organizations. APIs, if not properly secured, can increase the risk of data breaches and privacy violations, requiring constant vigilance and robust safeguards.

In practice, inconsistencies in API standards and documentation can make integration difficult, slowing down adoption and creating headaches for developers. The transition to API-first systems can also disrupt existing workflows, requiring new training and administrative processes that may frustrate staff and slow down operations.

Additionally, some organizations may introduce unnecessary barriers to API access, whether intentionally or not, undermining the goal of seamless data exchange. If APIs are poorly implemented or inconsistently enforced, trust in certified health IT can suffer, ultimately impacting patient care.

c. How could ASTP/ONC revise health IT certification criteria to require APIs to consistently support exchanging data from all aspects of the patient's chart (for example, faxed records, free text, discrete data)?

To ensure APIs consistently support exchanging all aspects of a patient's chart (including faxed records, free text, and discrete data) ASTP/ONC could revise certification criteria to explicitly require access to the full range of clinical data types. This would involve mandating support for both structured data and unstructured content like scanned documents and clinical notes, using standardized FHIR resources such as Document Reference and Binary. Certification should prohibit excluding any data type and require clear, up-to-date documentation of API capabilities. Tying these requirements to information blocking rules would strengthen compliance and promote transparency. Additionally, leveraging SMART on FHIR and current implementation guides would help ensure secure, comprehensive, and user-friendly data exchange. Regular updates to certification criteria would keep pace with evolving standards and real-world needs, ultimately enabling more complete and seamless access to patient health information for providers, patients, and authorized applications.

d. What policy changes could CMS make so providers are motivated to respond to API-based data requests with best possible coverage and quality of data?

CMS could motivate providers to respond to API-based data requests with the best possible coverage and data quality by aligning incentives, strengthening requirements, and supporting providers with technical and administrative resources.

One of the most effective approaches would be to directly tie provider reimbursement, participation in value-based care models, or quality reporting programs to the completeness and timeliness of their API data responses. Namely, CMS could create new payment incentives or performance measures that reward providers who consistently deliver comprehensive, high-quality data through APIs.

CMS could also update certification and compliance requirements to ensure that providers' systems are technically capable of sharing all relevant data types via standardized APIs and require regular reporting on API usage and data quality metrics. Public reporting of these metrics would increase transparency and encourage providers to improve their performance.

Additionally, CMS can reduce the administrative burden by investing in technical assistance, data literacy training, and user-friendly data tools, as outlined in the CMS Innovation Center's data-sharing strategy. Providing clear guidance, robust implementation resources, and ongoing support would help providers overcome technical and workflow challenges, making it easier to respond to API-based requests with complete and accurate data.

By combining financial incentives, regulatory requirements, transparent reporting, and practical support, CMS can create an environment where providers are both motivated and empowered to deliver the highest quality data through APIs.

e. How could EHRs capable of bulk data transfer be used to reduce the burden on providers for reporting quality performance data to CMS? What capabilities are needed to show benefit? What concerns are there with this approach?

EHRs capable of bulk data transfer can significantly reduce the burden on providers for reporting quality performance data to CMS by automating the extraction and submission of large volumes of clinical data. Instead of manually compiling and submitting quality measures, providers can use standardized APIs (like FHIR Bulk Data) to efficiently transmit comprehensive, longitudinal patient data directly from their EHRs. This approach not only saves time and administrative effort but also improves the accuracy and completeness of quality reporting since it draws from all available patient records rather than just isolated data within a single system.

To realize these benefits, EHRs need robust capabilities: they must support standardized bulk data export, ensure data completeness across care settings, and provide valid, reliable, and easily extractable quality measure data. The system should also be able to integrate data from multiple sources, handle longitudinal records, and maintain compliance with privacy and security standards.

Practically, the Administration should take steps to end information blocking practices that are actively harming patients, with a focus on EHR developers who view information blocking as a competitive advantage. While we appreciate the resources created thus far by HHS, it is critical that the Administration acknowledges that existing rules addressing information blocking are not consistently being followed due in large part to a lack of enforcement. While some are implicitly violating the rules (e.g., offering "compliant" information exchange mechanisms that do not work in practice while offering functional solutions in parallel for a fee), others are unapologetically ignoring the rules. We emphasize that enforcement should be meaningful so as not to be viewed as a mere cost of doing business. If the Administration is going to accomplish its goal of overcoming barriers to the seamless exchange of health information across systems, it should first make immediate efforts to resolve information blocking complaints, publish its findings, and take action on them to ensure that a baseline of data exchange is occurring. Enforcement should contribute to a predictable environment while taking into consideration the severity of the alleged misconduct so as to avoid disproportionate impacts.

There are other challenges. For example, not all EHRs may capture every data element needed for quality measures, especially if care is fragmented across multiple systems. Data standardization and interoperability challenges persist, and ensuring data quality and validity across diverse sources can be difficult. There are also technical and resource barriers to implementing bulk data capabilities, particularly for smaller providers.

TD-10. For EHR and other developers subject to the ONC Health IT Certification Program, what further steps should ASTP/ONC consider to implement the 21st Century Cures Act's API condition of certification (42 U.S.C. 300jj-11(c)(5)(D)(iv)) that requires a developer's APIs to allow health information to be accessed, exchanged, and used without special effort, including providing access to all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws?

To fully realize the 21st Century Cures Act's API certification requirement, ASTP/ONC should ensure that certified APIs provide seamless access to all patient health data, including both structured and unstructured elements, while complying with privacy laws. This means mandating comprehensive data coverage, minimizing technical barriers like unnecessary registration, and enforcing standardized implementation guides such as SMART App Launch v2 for consistent, secure interoperability. Developers should be required to publish and maintain up-to-date API endpoint information to simplify discovery and connection. Additionally, HHS should strengthen monitoring and auditing to ensure ongoing compliance, linking these requirements firmly to information blocking enforcement. These steps will help provide APIs with truly enable easy, comprehensive, and reliable access to electronic health records, fulfilling the intent of the Cures Act.

CHI notes its significant concerns with proposals to privilege, licensed health care providers and exclude all other providers of healthcare services in creating a two tiered system where providers who are subject to federal privacy and security laws but are not licensed health care professionals as defined in TEFCA Standard Operating Procedures will have to undertake actions above and beyond those taken by licensed health care providers to ensure that their queries for patient health information for treatment are responded to and not blocked. The creation of such a dynamic is counter to the Cures Act requirement that "special effort" not be required. In addition, by artificially siloing data from digital-first health care providers, the proposed rule severely hampers the access, exchange, and use of a growing subset of electronically accessible health information by the full ecosystem of providers in the interest of patients, as we'll discuss below regarding impact.

CHI is also concerned with ASTP's decision during the previous Administration to outsource significant policy decisions under the Trusted Exchange Framework and Common Agreement to third parties who did not engage in adequate consultations with impacted stakeholder communities before setting deeply impactful policies. Such decisions should be subject to notice and comment periods.

CHI further has concern with ASTP's decision to implement AI transparency reporting requirements for "predictive decision support intervention" AI in the electronic healthcare record space, which were adopted pursuant to the previous Administration's AI Executive Order. These reporting requirements overlap with existing requirements, and we urge for their withdrawal (or at minimum, their conversion into voluntary reporting measures).

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?**

CHI would support EHI export capabilities being revised to specify standardized API requirements. Currently, health IT developers have flexibility in how EHI export is implemented, which supports innovation but leads to inconsistent formats and methods across systems. This variability can create barriers to interoperability, complicate data integration, and increase the burden on providers and patients who need to use or share exported health information. By specifying standardized API requirements, such as mandating the use of widely adopted formats like FHIR for both single-patient and population-level exports, ONC would ensure that EHI exports are consistent, computable, and easier to integrate across different platforms. Standardized APIs would also enable more seamless, automated, and secure data exchange, supporting the broader goals of interoperability and information blocking prevention.

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

Yes, there are specific workflow aspects of EHI export that could be improved through standardization and thoughtful design. Currently, workflows for EHI export can be inconsistent and burdensome for both patients and administrative staff. Patients often face challenges locating export options, managing large files, and navigating different processes across health systems. Administrative staff may need to manually review, attach, or redact records, adding to their workload and introducing delays.

Standardizing EHI export through APIs, such as using FHIR-based approaches, can streamline these workflows. For patients, user-friendly web or mobile applications could allow them to easily request, track, and download their health information from multiple providers in one place, reducing confusion and manual effort. Automated status updates and clear interfaces can further simplify the process.

For administrators, integrated export management tools can help efficiently track requests, upload necessary attachments, and approve or reject exports within a unified system, minimizing manual steps and making the process more transparent and manageable.

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

Currently, while health IT developers must offer EHI export, the method is left to their discretion, resulting in inconsistent approaches and formats that can hinder interoperability and increase administrative burden. By aligning CMS program requirements, such as those in the Promoting Interoperability Program and related quality reporting initiatives, with standardized API requirements for EHI export, CMS can drive more uniform, computable, and automated data exchange.

Policy changes could include:

- Requiring support for API-based, standards-driven EHI export for both individual and population-level data.

- Integrating the use of these APIs into performance measures, reporting objectives, or attestation requirements within CMS programs, making their use a condition for full program participation or scoring.
- Providing technical guidance and incentives for the adoption of API-based workflows, reducing manual steps for patients and providers and ensuring timely, high-quality data exchange.

4. Data Exchange

TD-12. Should CMS endorse non-CMS data sources and networks, and if so, what criteria or metrics should CMS consider?

CHI notes its support for CMS' acknowledgment that the use of health IT past CEHRT offers the ability to improve care and keep patients safe. We urge that CMS move away from its reliance on CEHRT (through, for example, permitting health IT that builds on top of CEHRT) in order to provide increased competition in the marketplace as well as greater flexibility and choice to providers and patients. CHI notes its support of 2015 CEHRT requirements in 2019, but we reiterate our concern with, and lack of confidence in, any presumption that the 2015 ONC CEHRT standards will facilitate seamless interoperability.

CMS should consider endorsing non-CMS data sources and networks to strengthen interoperability and improve access to health information, as long as these sources meet high standards for quality, security, and reliability. To do this, CMS could evaluate potential partners based on criteria such as data accuracy and completeness, compliance with privacy and security regulations, use of national interoperability standards like FHIR, and broad network participation. Additionally, CMS should look for strong performance, transparency, and effective governance. By setting and applying these benchmarks, CMS can responsibly expand its network of trusted data partners, supporting better care coordination and outcomes for patients.

TD-13. What new opportunities and advancements could emerge with APIs providing access to the entirety of a patient's electronic health information (EHI)?

APIs that provide access to the entirety of a patient's electronic health information (EHI) open up significant new opportunities and advancements in healthcare. With full EHI access, patients, providers, and authorized third parties could benefit from comprehensive, longitudinal health records, enabling more personalized care, advanced analytics, improved care coordination, and streamlined administrative processes. Real-time access to all EHI could also drive innovation in digital health tools, support population health management, and enhance research capabilities.

a. **What are the primary obstacles to this?**

The main obstacles to providing API access to full EHI include:

- **Data Standardization and Quality:** Unlike the USCDI, which is a defined and structured set of data elements, full EHI encompasses a wide range of clinical and administrative data, much of which is unstructured, inconsistently coded, or stored in proprietary formats. This makes reliable extraction, exchange, and interpretation challenging.
- **Technical Complexity:** EHR systems may not be uniformly equipped to expose all EHI via APIs, especially for legacy data or custom fields not mapped to standard vocabularies.
- **Privacy and Security:** Broader data sharing increases the risk of unauthorized access or breaches, requiring robust consent management, authentication, and audit capabilities.
- **Information Overload:** Providing access to the entirety of EHI may overwhelm users and systems with irrelevant or low-value data, complicating clinical workflows and decision-making.

b. What are the primary tradeoffs between USCDI and full EHI, especially given more flexible data processing capabilities today?

The tradeoffs between using USCDI and providing access to the entirety of a patient's electronic health information (EHI) revolve around scope, standardization, and practical utility. USCDI offers a defined, standardized set of data elements that are widely supported by EHR systems and ensure a consistent, reliable foundation for interoperability. This approach makes it easier for providers, payers, and patients to exchange essential health information efficiently and securely, with lower risk of privacy breaches or information overload.

In contrast, granting API access to full EHI opens the door to much broader and more flexible data use. This can foster innovation, support advanced analytics, and enable more personalized care and research by making all available health data accessible. However, this expanded access comes with significant challenges. Full EHI often includes unstructured or proprietary data that may not be consistently coded or easily interpreted, increasing the technical complexity of data exchange. There are also heightened privacy and security risks, as well as the potential for overwhelming users and systems with large volumes of less relevant information.

Ultimately, while USCDI ensures a manageable and interoperable core dataset, full EHI access provides greater flexibility and potential for innovation, but at the cost of increased complexity, variability, and risk. The choice between these approaches depends on balancing the need for reliable, standardized data exchange with the desire to unlock the full potential of comprehensive health information.

TD-14. Regarding networks' use of FHIR APIs:

a. **How many endpoints is your network connected to for patient data sharing? What types, categories, geographies of endpoints do you cover? Are they searchable by National Provider Identifier (NPI) or organizational ID?**

FHIR networks can be connected to thousands of endpoints for patient data sharing. These endpoints span a wide range of types, including clinical EHRs, payers, and provider organizations, and cover diverse geographies across the U.S. and beyond. Endpoints are typically searchable by National Provider Identifier (NPI) or organizational ID, especially when leveraging national directory standards and APIs.

b. **How are these connections established (for example, FHIR (g)(10) endpoints, TEFCA/Integrating the Health Enterprise (IHE) XCA, or proprietary APIs)?**

Connections are established using a variety of mechanisms including:

- **FHIR (g)(10) Endpoints:** Standards-based endpoints required for certified EHR technology, supporting RESTful API access to patient data.
- **Population-Level Endpoints:** These endpoints enable sharing data for groups of patients, often under B2B agreements, without individual patient authentication.
- **Patient-Mediated Endpoints:** These require patient authentication and consent for data sharing.
- **Other Standards and Proprietary APIs:** Some networks also use TEFCA/IHE XCA protocols or proprietary APIs for specific use cases or legacy integration needs.

c. **Do you interconnect with other networks? Under what frameworks (for example, TEFCA, private agreements)?**

Many FHIR networks interconnect with other networks to expand reach and data liquidity. These interconnections are established under frameworks such as TEFCA, which provides a national trust framework for secure data exchange, or through private agreements between organizations. This interoperability allows networks to aggregate and share clinical and claims data across a broad ecosystem, supporting both patient-mediated and population-level data exchange.

TD-15. Regarding bulk FHIR APIs:

a. **How would increased use of bulk FHIR improve use cases and data flow?**

Bulk FHIR APIs enable efficient, standardized extraction and transfer of large volumes of healthcare data, supporting population-level use cases such as public health reporting, population health management, clinical research, payer-to-payer data exchange, and advanced analytics. They allow for asynchronous, high-performance data transfers, reducing latency and manual effort

compared to serial, record-by-record API calls. Bulk FHIR APIs simplify integration and interoperability, making it easier for authorized users, such as providers, payers, and public health agencies, to access complete, accurate, and timely data for entire patient populations. The approach supports regulatory compliance (e.g., ONC and CMS interoperability rules), reduces costs associated with custom data interfaces, and enables better-informed clinical and operational decisions.

b. What are the potential disadvantages of their use?

Extracting and processing large datasets can strain system resources, requiring robust infrastructure and careful management of performance, storage, and security. Data quality and standardization issues may arise, as not all EHRs or data sources consistently structure or code information, potentially leading to errors or incomplete data. Privacy and security risks increase with the movement of large volumes of sensitive health data, making strong access controls, logging, and compliance measures essential. There is potential for information overload, where users or systems may be overwhelmed by the volume of data, complicating analysis and actionable insights. Implementation complexity can be difficult, especially for organizations with legacy systems or limited technical expertise.

TD-16. What are the tradeoffs of maintaining point-to-point models vs. shared network infrastructure?

Point-to-point models create dedicated, direct connections between specific locations or systems. Their main advantages are enhanced security, reliability, and performance, data travels on exclusive pathways, reducing exposure to external threats and ensuring real-time access, which is crucial for sensitive patient information and compliance with regulations like HIPAA. These models are particularly effective for high bandwidth needs such as medical imaging or telemedicine, and they simplify security management by limiting the number of access points. However, as networks grow, point-to-point integrations become increasingly complex, expensive, and difficult to scale. Each new connection requires custom development and maintenance, resulting in a tangled web that can hinder broader interoperability and slow innovation.

Shared network infrastructure, such as health information exchanges or networks built on standardized APIs, enables multiple participants to access and exchange data through a common platform. This approach supports scalability, reduces redundant integration efforts, and fosters broader interoperability across organizations. Shared infrastructure can lower costs, streamline onboarding, and make it easier to implement new standards or regulatory requirements. However, it may introduce new security and privacy challenges, as data is transmitted over shared pathways, and requires robust governance to ensure trust and compliance.

a. Do current rules encourage scalable network participation?

Current rules are increasingly pushing toward scalable, shared network participation by promoting standardized APIs and frameworks like TEFCA, but legacy regulations and reimbursement models still allow or even incentivize point-to-point connections in some cases. The transition is ongoing, and while policy momentum favors scalability, practical adoption varies.

b. What changes would improve alignment (for example, API unification, reciprocal access)?

To better align the healthcare ecosystem with scalable, interoperable data exchange, several policy and technical changes are needed. First, unifying APIs across networks would ensure that all participants are using the same open, standardized frameworks for data sharing, reducing fragmentation and making integration simpler and more predictable. Reciprocal access is also crucial because every organization connected to a network should be able to both send and receive data.

Additionally, streamlining the certification and onboarding process for shared infrastructure would lower barriers to participation, allowing more organizations to join networks quickly and efficiently. Finally, addressing privacy and security concerns with clear, enforceable standards tailored to shared environments would build trust and protect sensitive health information as it moves across broader networks. Together, these changes would create a more unified, scalable, and secure foundation for nationwide health data exchange.

TD-17. Given operational costs, what role should CMS or ASTP/ONC or both have in ensuring viability of healthcare data sharing networks, including enough supply and demand, that results in usage and outcomes?

CMS and ASTP/ONC have a critical role in ensuring the viability of healthcare data sharing networks, especially given the operational costs and the need to sustain both supply and demand for data exchange that leads to real usage and improved outcomes:

- Both can set foundational policy and technical standards, such as mandating open, standards-based APIs and supporting frameworks like TEFCA, to lower barriers to entry, reduce fragmentation, and ensure interoperability across networks. By establishing clear requirements and certification processes, CMS and ASTP/ONC can help networks avoid duplicative investments and ensure that both providers and payers can participate efficiently.
- Both can use their regulatory and purchasing power to align incentives, such as tying participation in value-based care models or federal programs to network usage, and designing both “carrots and sticks” to encourage robust data exchange. This may include financial incentives, public reporting, and penalties for those who do not participate or who block information sharing.
- Both can directly invest in or support shared infrastructure projects, like a national provider directory, digital identity solutions, or digital insurance cards, that make it easier for

networks to scale and for stakeholders to connect and use data. These investments help ensure that there is enough supply (networks and endpoints) and demand (providers, payers, patients) to create a thriving ecosystem.

- Both should foster ongoing collaboration with the private sector, regularly seek stakeholder input, and remain agile in updating policies and technical requirements as technology and market needs evolve. This approach helps networks remain viable, relevant, and capable of delivering meaningful health outcomes.

5. Compliance

TD-18. Information blocking:

a. **Could you, as a technology vendor, provide examples for the types of practices you have experienced that may constitute information blocking. Please include both situations of non-responsiveness as well as situations that may cause a failure or unusable response?**

As a technology vendor, we have experienced several types of practices that may constitute information blocking, including both non-responsiveness and actions that result in failure or unusable responses.

- Non-responsiveness:
    - Some organizations simply do not respond to requests for electronic health information (EHI), even after multiple follow-ups. This can include ignoring requests from patients, providers, or third parties authorized by the patient, without providing a valid reason or citing an allowable exception.
    - Delays in releasing EHI after a legitimate request can also be considered information blocking, particularly when there is no clear justification for the delay and it interferes with timely access to care or data exchange.
- Failure or Unusable Response:
    - In some cases, organizations provide data in non-standardized or proprietary formats that are difficult or impossible to use, even though more interoperable options are available.
    - Limiting the time window for access to requested information, such as providing a one-time link that expires within hours or days, can make the data practically unusable for the requester.
    - Charging excessive or unreasonable fees for data access or export, beyond what is permitted by HIPAA or other regulations, is another form of information blocking that can effectively prevent or discourage data exchange.
    - Imposing unnecessary restrictions on authorized users, such as refusing to enable patient or provider access to APIs or requiring burdensome manual processes for what could be automated data sharing, also constitutes information blocking.

b. What additional policies could ASTP/ONC and CMS implement to further discourage healthcare providers from engaging in information blocking practices?

To further discourage healthcare providers from engaging in information blocking, ASTP/ONC and CMS could take a more proactive and visible approach to enforcement, transparency, and provider support.

First and foremost, HHS should increase the frequency and public visibility of enforcement actions. By regularly publicizing penalties and maintaining a widely promoted public list of violators, CMS and ASTP/ONC can raise awareness and signal that information blocking will not be tolerated. Expanding beyond complaint-driven investigations, these agencies could also conduct targeted audits of providers' data sharing practices, particularly focusing on those with high patient volumes or histories of non-compliance.

Tying participation in broader federal programs and value-based payment models even more closely to compliance with information blocking rules would further motivate providers to prioritize open data exchange. At the same time, refining and clarifying the exceptions to information blocking would help reduce confusion and prevent providers from withholding information inappropriately.

Education and support remain crucial. By offering robust training, technical assistance, and clear policy templates, CMS and ASTP/ONC can help providers better understand their obligations and how to comply. Additionally, making it easier for patients, providers, and vendors to report suspected information blocking, and ensuring strong protections for whistleblowers, would encourage greater accountability.

CHI is also concerned with ASTP's decision during the previous Administration to outsource significant policy decisions under the Trusted Exchange Framework and Common Agreement to third parties who did not engage in adequate consultations with impacted stakeholder communities before setting deeply impactful policies. Such decisions should be subject to notice and comment periods.

CHI further has concern with ASTP's decision to implement AI transparency reporting requirements for "predictive decision support intervention" AI in the electronic healthcare record space, which were adopted pursuant to the previous Administration's AI Executive Order. These reporting requirements overlap with existing requirements, and we urge for their withdrawal (or at minimum, their conversion into voluntary reporting measures).

c. Are there specific categories of healthcare actors covered under the definition of information blocking in section 3022(a)(1) of the Public Health Service Act (PHSA) that lack information blocking disincentives?

Section 3022(a)(1) of the Public Health Service Act (PHSA) and its implementing regulations identify four main types of actors subject to the information blocking provision: health care providers,

health IT developers of certified health IT, health information exchanges (HIEs), and health information networks (HINs). For health IT developers, HIEs, and HINs, the statute prescribes civil monetary penalties of up to $1 million per violation for information blocking. However, for health care providers, the law specifies only "appropriate disincentives" rather than a set monetary penalty. While ONC and CMS have proposed and begun implementing certain disincentives for providers, such as exclusion from federal programs or public reporting, these measures are still being finalized and are not as direct or uniformly applied as the penalties for developers, HIEs, and HINs.

TD-19. Regarding price transparency implementation:

a. **What are current shortcomings in content, format, delivery, and timeliness?**
b. **Which workflows would benefit most from functional price transparency?**
c. **What improvements would be most valuable for patients, providers, or payers, including CMS?**
d. **What would further motivate solution development?**

The CHI community fully supports enhancing transparency. We believe that the use of digital health solutions enables eased implementation of transparency to detect trends in real time. Enhanced data tracking, collection, and analysis using AI tools can particularly assist in realizing value-based care goals (see our answers below).

Value-Based Care Organizations

1. Digital Health Adoption

VB-1. What incentives could encourage APMs such as accountable care organizations (ACOs) or participants in Medicare Shared Savings Program (MSSP) to leverage digital health management and care navigation products more often and more effectively with their patients? What are the current obstacles preventing broader digital product adoption for patients in ACOs?

CMS has an excellent opportunity to advance the American healthcare system by leveraging digital medical technologies, both those available today as well as emerging fields such as AI and enhanced data analytics. We urge CMS to utilize every opportunity available to move away from legacy technology systems and towards a truly connected continuum of care through its implementation of the QPP, consistent with the CHI's Value-Based Care Task Force recommendations.[17]

Despite the best efforts of CMS to increase the number of Advanced APMs, many providers in certain geographies, specialties, and practice settings lack viable options for APM participation over a decade since CMMI's inception, particularly when pro-digital health policies could incent the move to APMs. Moreover, CMMI's existing suite of Advanced APMs do not adequately embrace innovative technological healthcare delivery mechanisms. Value-based care models that are currently in place do not provide the flexibilities needed to incorporate the full range of virtual care modalities (except for voice/video) into digitally enabled care models and it is becoming increasingly evident that the goal of realizing value-based care is escaping, despite the efforts of public and private healthcare efforts.[18]

Moreover, CMMI models are typically only run for five years since CMMI must pilot test models before making them permanent. CMMI has sole authority to "expand" models for either permanent or wide geographic implementation if the model is expected to decrease spending without decreasing quality of care, or if the model is expected to increase quality without increasing spending. As of February 2021, CMMI tested 54 models; in 2020, CMMI was actively operating 24 payment and delivery models. Seven of these models received designation as Advanced APMs. Despite testing dozens of models, only four CMMI models have met the criteria for expansion into a nation-wide program, including only one Advanced APM, the Pioneer Accountable Care Organizations (ACO) model, which served as a model for one of the tracks in the MSSP program, the current Enhanced Track. Given the critical need for transformation of the American healthcare sector and the rapid development of new technologies that can contribute to CMS' value-based care mission, this process can be astonishingly slow. For the 2019 Quality Payment Performance Period, 195,564 eligible clinicians earned Qualifying APM Participant (QP) status while another

[17] https://www.connectedhi.com/blog/2021/7/14/the-value-based-care-revolution-will-stall-without-health-tech.

[18] Gondi et al, "REACHing" for Equity , Moving from Regressive toward Progressive Value-Based Payment, N Engl J Med 2022; 387:97-99, DOI: 10.1056/NEJMp2204749.

27,995 eligible clinicians earned partial QP status; in contrast, 954,614 eligible clinicians participated in MIPS in 2019.[19]

While CMS has long stated that its goal is for most providers to participate in APMs, rather than MIPS, this is far from realized and there are insufficient APM options for most specialists. The Physician-Focused Payment Model Technical Advisory Committee (PTAC),[20] charged with recommending new specialty-relevant APM models to CMS for testing under CMMI, has to date received and evaluated 39 proposed APMs and recommended that HHS take action on 28 of them.[21] While PTAC has authority to recommend models to CMMI to pilot test, its authority is merely advisory as CMMI has sole authority to test, implement, and expand APMs. Congress envisioned that the PTAC would help accelerate the development of new Advanced APM options, which could be exploring new digital health-driven efficiencies and ways to bring greater quality into the care continuum while reducing costs. However, HHS has not, to date, adopted a single PTAC-recommended model for testing. CMMI leadership has acknowledge that, after 10 years, not enough progress has been made in successfully shifting to value-based care.[22]

CHI supports CMS' explicitly endorse the use of digital medical technologies in both MIPS and APMs. CHI supports Congress' goal of realizing innovative APMs and continues to work with stakeholders to find eligible alternatives to MIPS. APMs, with their financial and operational incentives, demonstrate the best uses of digital health tools. Because providers who practice in APMs are often judged on their ability to control patients' total spending, they have a natural constraint on fraud, abuse, and overuse that digital health's use might be susceptible to in a pure fee-for-service system.

To date, CMS has not discussed digital health tools' key role in the success of APMs which should have the flexibility to use connected health technologies for patients with specific at-risk chronic conditions. For example, the MSSP, by far Medicare's largest APM, CMS only waives patient location and geographic limitations on accountable care organizations (ACOs) that are at financial risk and use prospective assignment. There also haven't been case studies on ACOs' use of RPM. In order to help providers utilizing APMs meet statutory requirements to reduce total costs, CMS should exercise its statutory authority under 42 U.S.C. 1315a(d)(1) (in the case of CMMI Models) and 42

---

[19] Medicare Program; CY 2021 Payment Policies Under the Physician Fee Schedule and Other Changes to Part B Payment Policies; Medicare Shared Savings Program Requirements; Medicaid Promoting Interoperability Program Requirements for Eligible Professionals; Quality Payment Program; Coverage of Opioid Use Disorder Services Furnished by Opioid Treatment Programs; Medicare Enrollment of Opioid Treatment Programs; Electronic Prescribing for Controlled Substances for a Covered Part D Drug; Payment for Office/ Outpatient Evaluation and Management Services; Hospital IQR Program; Establish New Code Categories; Medicare Diabetes Prevention Program (MDPP) Expanded Model Emergency Policy; Coding and Payment for Virtual Check-in Services Interim Final Rule Policy; Coding and Payment for Personal Protective Equipment (PPE) Interim Final Rule Policy; Regulatory Revisions in Response to the Public Health Emergency (PHE) for COVID–19; and Finalization of Certain Provisions from the March 31st, May 8th and September 2nd Interim Final Rules in Response to the PHE for COVID–19, 85 Fed. Reg. 84472 (Dec. 28, 2020).

[20] https://aspe.hhs.gov/ptac-physician-focused-payment-model-technical-advisory-committee

[21] https://aspe.hhs.gov/proposal-submissions-physician-focused-payment-model-technical-advisory-committee

[22] E.g., https://podcasts.apple.com/us/podcast/health-for-all/id1530836259?i=1000548550683.

U.S.C. 1395jjj(f) (in the case of the MSSP) to waive payment and program requirements as appropriate. Specifically, CMS should allow wider use of telehealth in the MSSP by allowing all ACOs access to telehealth waivers and expand what telehealth waivers cover, for example, to include patient cost-sharing, modalities, and covered services.

CMS should also waive payment and program requirements as appropriate to provide flexibility for use of digital health innovations in APMs. Congress has already granted CMS broad authority to implement telehealth use in APMs, but the agency has so far been reluctant to allow its use. For example, Medicare provides telehealth waivers for two-sided ACOs who use prospective attribution. But this limits telehealth's use to a mere 17 percent of ACOs in the MSSP. Instead, all ACOs, regardless of risk selection or use of attribution, should enjoy this flexibility.

VB-2. How can key themes and technologies such as artificial intelligence, population health analytics, risk stratification, care coordination, usability, quality measurement, and patient engagement be better integrated into APM requirements?

Key themes and technologies, such as artificial intelligence, population health analytics, risk stratification, care coordination, usability, quality measurement, and patient engagement, can be better integrated into Alternative Payment Model (APM) requirements by making them central to both the design and evaluation of these models.

APMs should explicitly endorse and incentivize the use of advanced analytics and AI to identify high-risk patients, stratify populations, and support proactive care interventions. Integrating population health tools and risk stratification into provider workflows enables more targeted, efficient care and helps meet quality and cost goals. Care coordination should be incentivized through APMs by rewarding data sharing, team-based care, and seamless transitions across settings, supported by interoperable health IT and real-time data exchange.

Usability and patient engagement can be advanced by incentivizing that APM participants use digital tools that are intuitive, accessible, and support patient self-management and shared decision-making. Quality measurement should move toward automated, real-time reporting using standardized data, reducing administrative burden and enabling continuous performance feedback.

To ensure successful integration, APM requirements should include clear standards for technology adoption, data transparency, and provider support, such as training, benchmarking, and workflow integration, so that these tools translate into actionable insights at the point of care. By aligning payment incentives, regulatory requirements, and technology standards, APMs can fully leverage these innovations to drive better outcomes, efficiency, and patient experience.

Further, CHI has worked to proactively address health AI governance and policy issues based on consensus views that span the healthcare sector, from technology developers to providers to patients, and we urge for alignment with:

- **T**he CHI community's Health AI Policy Principles (https://connectedhi.com/wp-content/uploads/2022/02/Policy-Principles-for-AI.pdf);

- CHI recommendations on advancing transparency for AI in the healthcare ecosystem (https://connectedhi.com/wp-content/uploads/2022/02/AdvancingTransparencyforArtificialIntelligenceintheHealthcareEcosystem.pdf);
- CHI's AI Roles and Interdependencies Framework (https://connectedhi.com/wp-content/uploads/2024/02/CHI-Health-AI-Roles.pdf); and
- CHI's recommendations to the Department on Government Efficiency on ways to use AI to improve healthcare governance efficiency (https://connectedhi.com/wp-content/uploads/2025/01/CHI-DOGE-Recommendations-30-Jan-2025.pdf).

VB-3. What are essential health IT capabilities for value-based care arrangements?

a. **Examples (not comprehensive) may include: care planning, patient event notification, data extraction/normalization, quality performance measurement, access to claims data, attribution and patient ID matching, remote device interoperability, or other patient empowerment tools.**

For value-based care arrangements, essential health IT capabilities include tools that support coordinated, data-driven, and patient-centered care. This means having systems for real-time care planning and communication among care teams, as well as event notifications to alert providers about key patient events like hospital admissions or discharges. Robust data integration and normalization are crucial for creating a complete patient record, while automated quality measurement tools help track and improve outcomes with less administrative effort.

Access to both clinical and claims data gives providers a comprehensive view of patient care and costs, and accurate patient matching ensures the right data is linked to the right individuals. Interoperability with remote monitoring devices enables proactive management of chronic conditions, while patient empowerment tools, such as portals and remote patient monitoring innovations, encourage engagement and shared decision-making. Finally, analytics, decision support, and real-time dashboards help identify care gaps and monitor key performance metrics, all of which are vital for delivering high-quality, cost-effective care in value-based models.

b. **What other health IT capabilities have proven valuable to succeeding in value-based care arrangements?**

Further health IT capabilities have proven valuable for success in value-based care arrangements:

- **Advanced Interoperability Solutions:** Seamless data exchange between payers, providers, and other care partners enables real-time access to actionable information, which is crucial for coordinated, patient-centered care.
- **AI-Driven Risk Stratification and Predictive Analytics:** Artificial intelligence and sophisticated analytics help identify high-risk patients, close care gaps, and support proactive interventions, ultimately improving outcomes and resource allocation.

- **Automated Workflow and Care Management Tools:** Platforms that automate care coordination, documentation, and compliance monitoring reduce administrative burden and allow providers to focus more on patient care.
- **Integrated Patient Engagement Platforms:** Mobile apps, portals, and virtual agents facilitate communication, support care plan adherence, and empower patients to participate actively in their health management.
- **Remote Monitoring and Home-Based Care Technology:** Tools that support care delivery outside traditional settings enable continuous monitoring and timely interventions, especially for chronic disease management and post-acute care.
- **Real-Time Performance Dashboards and Analytics:** Integrated dashboards provide up-to-date insights on quality, utilization, and financial metrics, supporting continuous improvement and strategic decision-making.
- **Point-of-Care Decision Support:** Clinical decision support tools nudge providers toward evidence-based care pathways, optimize referrals, and enhance coding accuracy, directly impacting quality and cost outcomes.
- **Data Integration and Aggregation Platforms:** Solutions that unify data from disparate sources, EHRs, claims, labs, devices, create a holistic view of the patient journey, enabling more effective population health management.

VB-4. What are the essential data types needed for successful participation in value-based care arrangements?

To succeed in value-based care arrangements, organizations need access to a comprehensive range of data types. This includes detailed clinical information from electronic health records, claims data that reveal patterns in utilization and costs, and social determinants of health that influence patient risk and outcomes. Demographic details, clinical risk scores, and care coordination records are also essential for identifying high-risk patients and ensuring continuity of care. Additionally, quality and outcome metrics, along with patient engagement data such as portal usage and patient-reported outcomes, help drive performance improvement and support shared decision-making. Together, these data types provide the foundation for effective risk management, care coordination, and quality measurement in value-based care models.

2. Compliance and Certification

VB-5. In your experience, how do current certification criteria and standards incorporated into the ONC Health IT Certification Program support value-based care delivery?

The ONC Health IT Certification Program supports value-based care by promoting interoperability, standardized data, and transparency. It requires health IT systems to use FHIR-based APIs and incorporate the USCDI data set, enabling seamless access to comprehensive patient information across settings. This facilitates care coordination, population health management, and quality

measurement. The program also enforces information blocking rules and includes standards for AI-driven decision support and public health reporting, helping providers identify high-risk patients and improve outcomes.

Despite setting important baseline standards, the ONC Health IT Certification Program falls short in fully supporting value-based care. Its criteria often focus on minimum requirements, leaving out advanced capabilities like robust analytics, comprehensive care coordination, and seamless integration of diverse data types such as social determinants of health and patient-reported outcomes. Certification is based on lab testing rather than real-world performance, so systems may not function optimally in practice, especially when handling complex workflows or data from multiple sources. The program's slow update cycle and emphasis on administrative compliance can add burden without directly advancing value-based care goals. Additionally, because participation is voluntary, adoption remains uneven, leading to persistent gaps in interoperability and functionality across the healthcare system.

VB-6. What specific health information technology capabilities that could benefit APMs are not currently addressed by existing certification criteria and standards that should be included under the ONC Health IT Certification Program?

Several health IT capabilities that are critical for Alternative Payment Models (APMs) are not fully addressed by current ONC Health IT Certification Program criteria and standards, but should be considered for inclusion:

- **Advanced Population Health Analytics:** While current certification ensures basic interoperability and data exchange, it does not require sophisticated analytics tools that aggregate and analyze data across populations to identify high-risk patients, predict outcomes, and support proactive interventions, capabilities central to value-based care.
- **Comprehensive Care Coordination Tools:** Existing standards do not mandate features that facilitate closed-loop referrals, real-time care team communication, or longitudinal care planning across multiple organizations, all of which are essential for managing complex patient populations in APMs.
- **Social Determinants of Health (SDoH) Integration:** Certification criteria do not comprehensively address the capture, exchange, and use of SDoH data, which are increasingly recognized as vital for risk assessment, care planning, and addressing health disparities in value-based models.
- **Patient-Reported Outcomes and Engagement Data:** There is limited requirement for systems to collect, exchange, and utilize patient-reported outcomes or engagement metrics, which are important for measuring quality and supporting patient-centered care.
- **Attribution and Patient Matching:** Accurate patient attribution and ID matching across disparate data sources are not standardized under current certification but are critical for assigning patients to providers and tracking outcomes in APMs.
- **Integration with Claims and Non-Traditional Data Sources:** Certification focuses primarily on clinical data, with limited requirements for integrating claims, pharmacy,

behavioral health, and community-based data, all of which are necessary for a holistic view of patient care and costs.

- **Automated Quality Measurement and Reporting:** While quality reporting is supported, automated, real-time quality measurement using standardized digital measures is not universally required, limiting timely performance feedback and improvement.
- **AI-Enabled Decision Support:** Current standards do not require or test for advanced, AI-driven clinical decision support tools that can help providers close care gaps, optimize resource use, and improve outcomes.

Including these capabilities in ONC certification criteria would better align health IT with the needs of APMs and value-based care, ensuring providers have the tools necessary to deliver coordinated, high-quality, and cost-effective care.

VB-7. How can technology requirements for APMs, established through CEHRT or other pathways, reduce complexity while preserving necessary flexibility?

Technology requirements for APMs, whether established through CEHRT or other pathways, can reduce complexity while preserving flexibility by setting clear, foundational standards that all participants must meet, but allowing room for innovation in how those standards are achieved. For example, current APM criteria require the use of certified EHR technology (CEHRT) and alignment with evidence-based quality measures. This ensures a consistent baseline for data exchange, quality reporting, and care coordination, which simplifies participation and compliance across diverse providers.

At the same time, these requirements do not dictate the specific tools or workflows organizations must use, enabling providers to select solutions that best fit their unique clinical and operational needs. By focusing on outcomes, such as reliable data capture, interoperability, and quality measurement, rather than prescribing detailed technical implementations, APMs can encourage adoption of best practices while supporting local flexibility and innovation.

Additionally, maintaining a modular approach to certification allows providers to adopt new functionalities as their needs evolve, without overhauling entire systems. This balance of standardization and adaptability helps lower administrative burden, streamlines integration across care settings, and supports the diverse strategies necessary for success in value-based care.

VB-8. How can other HHS policies supplement CEHRT requirements to better optimize the use of digital health products in APMs? As an example, requirements under the Conditions of Participation for hospitals (42 CFR 482.24(d)) require hospitals to transmit electronic patient event notifications to community providers. What barriers are in place preventing APM participants from receiving the same notifications?

HHS policies can play a crucial role in supplementing CEHRT requirements to optimize the use of digital health products in APMs, especially by expanding standards for interoperability and event

notifications. Currently, hospitals are required to send electronic patient event notifications to community providers, but this requirement does not extend to all APM participants, such as clinicians in outpatient settings or accountable care organizations. As a result, many APM participants are left without timely alerts about important patient events like admissions or discharges.

Several barriers contribute to this gap. The existing regulations are limited in scope, applying only to hospitals and not to the broader network of providers involved in APMs. There's also a lack of standardized, interoperable infrastructure to ensure notifications reach all relevant parties, and not all APM participants have health IT systems capable of receiving these alerts. Additionally, issues like information blocking and privacy concerns can further restrict the flow of information.

To close these gaps, HHS could broaden event notification requirements to include all APM participants, promote the adoption of interoperable digital health tools across care settings, and clarify policies to minimize information blocking. These steps would help ensure that everyone involved in value-based care has timely access to critical patient information, ultimately supporting better care coordination and improved patient outcomes.

VB-9. What technology requirements should be different for APM organizations when comparing to non-APM organizations (for example, quality reporting, and interoperability)?

APM organizations may need to have different, more targeted technology requirements than non-APM organizations, especially in areas like quality reporting and interoperability. APM technology requirements should account for the following:

- For quality reporting, APM organizations, such as those participating in Advanced APMs or Medicare Shared Savings Program ACOs, are required to use Certified EHR Technology (CEHRT) that meets ONC standards and must report on quality measures comparable to or more robust than those required under MIPS. Starting in 2025, all APM participants must use CEHRT for quality reporting and make Promoting Interoperability submissions, ensuring that data is standardized and comparable across organizations. In contrast, non-APM organizations may have lower thresholds for CEHRT adoption and can often choose from a broader range of reporting mechanisms with less stringent requirements.
- In terms of interoperability, APM organizations must demonstrate advanced capabilities, such as bidirectional data exchange, real-time event notifications, and the use of FHIR-based APIs and the US Core Data for Interoperability (USCDI) standards. These requirements are designed to support care coordination, population health management, and seamless information sharing across care settings. Non-APM organizations, by comparison, often have fewer or less prescriptive interoperability mandates, which can result in inconsistent data sharing and less effective care coordination.

VB-10. In the Calendar Year (CY) 2024 Physician Fee Schedule final rule (88 FR 79413), CMS established that CEHRT requirements for Advanced APMs beyond those in the "Base EHR" definition should be flexible based on what is applicable to the APM that year based on the

area of clinical practice. What certification criteria should CMS identify under this flexibility for specific Advanced APMs, or for Advanced APMs in general? Are there specific flexibilities or alternatives to consider for smaller or resource-constrained (such as rural) providers in meeting CEHRT requirements without compromising quality of care or availability of performance data?

CMS's flexible approach to CEHRT requirements for Advanced APMs allows tailoring beyond the "Base EHR" definition based on each model's clinical focus and goals. Certification criteria should align with the specific needs of the APM, such as modules supporting relevant quality measure reporting, interoperability functions like FHIR-based APIs and event notifications, clinical decision support tailored to the specialty, care coordination capabilities, and social determinants of health data when applicable.

For smaller or resource-constrained providers, including those in rural areas, CMS should consider flexibilities like permitting the use of certified health IT modules instead of full EHR systems, allowing third-party intermediaries to meet certain requirements, offering shortened reporting periods, and providing technical assistance and financial support. This approach ensures that providers can meet quality and performance standards without undue burden, promoting equitable participation while maintaining the integrity of value-based care delivery.

3. Technical Standards

VB-11. What specific interoperability challenges have you encountered in implementing value-based care programs?

Implementing value-based care programs has revealed several persistent interoperability challenges. A major issue is the lack of seamless data exchange between disparate electronic health record (EHR) systems, which makes it difficult for providers to access comprehensive patient information across care settings. Many organizations struggle with integrating clinical, financial, and operational data into unified platforms, which is essential for effective care coordination, risk stratification, and population health management. This fragmentation hampers the ability to measure outcomes, identify care gaps, and drive improvements throughout the patient journey.

Another significant barrier is the limited adoption of standardized data formats and real-time data sharing, especially between payers and providers. Without robust interoperability solutions, value-based care models cannot fully leverage advanced analytics or AI-driven tools that depend on timely and accurate data. Smaller or rural providers often face additional hurdles due to high technology costs and limited resources for upgrading their IT infrastructure.

The lack of strong enforcement of information blocking regulations also contributes to these challenges. When organizations are not held accountable for withholding data, it further restricts the flow of critical information needed for value-based care, undermining efforts to improve outcomes and reduce costs. As a result, addressing interoperability gaps and ensuring compliance with information sharing requirements remain top priorities for advancing value-based care success.

VB-12. What technology standardization would preserve program-specific flexibility while promoting innovation in APM technology implementation?

Technology standardization for APMs should focus on establishing foundational requirements, such as the use of certified EHR technology, adoption of standardized data formats (like FHIR and USCDI), and robust quality measure reporting, while allowing flexibility in how these standards are implemented to fit the unique needs of each program or clinical setting. This approach ensures that all APMs can reliably exchange essential health information and report on outcomes, while still having the freedom to innovate with specialized tools or workflows that best support their patient populations or care models.

For example, CMS could require all APMs to support core interoperability standards and quality reporting mechanisms, but allow each program to select additional certified modules or functionalities that align with their clinical priorities, such as care coordination tools for primary care models or advanced analytics for specialty care. This modular strategy preserves program-specific flexibility and encourages the adoption of innovative solutions, while still maintaining a consistent technological foundation across APMs.

Standardizing critical data exchange and reporting elements while permitting customization beyond those minimums is a challenge, but promotes both interoperability and innovation, enabling APMs to evolve and address diverse healthcare challenges without unnecessary complexity or rigidity.

VB-13. What improvements to existing criteria and standards would better support value-based care capabilities while reducing provider burden?

To better support value-based care while reducing provider burden, health IT criteria and standards should focus on making data integration seamless, automating quality reporting, and requiring more robust interoperability. By adopting widely used standards like FHIR and USCDI, health IT systems can more easily aggregate data from EHRs, claims, and remote monitoring devices, streamlining care coordination and quality measurement. Automating digital quality reporting through tools like eCQMs would minimize manual data entry and free up providers to focus on patient care.

Additionally, standards should go beyond basic interoperability by mandating real-time data exchange and event notifications, ensuring information flows efficiently across all care settings. Allowing providers to use certified health IT modules tailored to their specific needs, rather than forcing them to adopt comprehensive systems, would also lower barriers for smaller and specialty practices. Finally, encouraging the integration of telehealth, patient portals, and AI-driven analytics would further enhance patient engagement and help providers identify care gaps more efficiently. These targeted improvements would enable value-based care models to thrive while minimizing the administrative workload for providers.

VB-14. How could implementing digital identity credentials improve value-based care delivery and outcomes?

Implementing digital identity credentials in healthcare has the potential to improve value-based care delivery and outcomes by enhancing data security, streamlining care coordination, and empowering both patients and providers. Digital credentials, such as verifiable credentials and digital wallets, allow patients to securely store and manage their health information, giving them control over what data is shared and with whom. This patient-centric approach reduces redundant paperwork, minimizes the risk of errors, and eliminates the need for repetitive tests, leading to a more efficient and coordinated care experience.

For providers, digital identity credentials ensure that patient interactions are consistently tied to a single, verified identity, which reduces fraud, improves the accuracy of patient records, and supports safer, more personalized care. These credentials also facilitate interoperability by enabling seamless, consent-based data sharing across different healthcare organizations and systems, which is essential for tracking outcomes and managing population health in value-based models.

Furthermore, digital identity verification streamlines administrative processes, such as onboarding and credentialing for staff, while strengthening compliance and reducing the risk of data breaches. By decentralizing data storage and allowing real-time updates, digital credentials protect sensitive health information and provide a resilient, unified framework for managing patient and provider identities.

VB-15. How could a nationwide provider directory of FHIR endpoints help improve access to patient data and understanding of claims data sources? What key data elements would be necessary in a nationwide FHIR endpoints directory to maximize its effectiveness?

A nationwide provider directory of FHIR endpoints could enhance access to patient data and understanding of claims data sources by serving as a centralized, validated repository of electronic endpoints for healthcare organizations, payers, and third-party applications. This directory would make it easier for providers, payers, and developers to find and connect with the correct FHIR endpoints, streamlining the process of exchanging clinical and claims information across the healthcare ecosystem. By reducing the need for each organization to independently identify, verify, and maintain endpoint connections, a national directory would lower administrative costs, minimize errors, and improve the timeliness and accuracy of data exchange.

Such a directory would also facilitate compliance with federal interoperability regulations and support better care coordination, decision-making, and patient outcomes by ensuring that the right data is accessible at the right time. It would also help clarify the sources of claims data, as each endpoint could be linked to specific organizations, services, and relationships, making data provenance and traceability much clearer.

To maximize its effectiveness, a nationwide FHIR endpoints directory should include key data elements such as:

- Organization and provider names and unique identifiers

- Endpoint URLs and technical details (e.g., FHIR version, supported resources)
- Capability statements describing the types of data and services available at each endpoint
- Contact information for endpoint administrators
- Relationships between providers, organizations, and services
- Accreditation or validation status to ensure trust and security
- Metadata on endpoint availability, reliability, and update history