June 16, 2025

The Honorable Robert F. Kennedy, Jr.
Secretary
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

Submitted electronically via http://www.regulations.gov

Dear Secretary Kennedy:

The Workgroup for Electronic Data Interchange (WEDI) writes today in response to the publication in the May 18, 2025, edition of the *Federal Register* entitled "Health Technology Ecosystem Request for Information" released by the Centers for Medicare & Medicaid Services (CMS) and the Assistant Secretary for Technology Policy, Office of the National Coordinator for Health Information Technology (ASTP/ONC), Department of Health and Human Services (HHS).

WEDI was formed in 1991 by then HHS Secretary Dr. Louis Sullivan to identify opportunities to improve the efficiency of health data exchange. WEDI was named in the HIPAA legislation as an advisor to the Secretary of HHS. Recognized and trusted as a formal advisor to the Secretary, WEDI is the leading multi-stakeholder authority on the use of health information technology (Health IT) to efficiently improve health information exchange, enhance care quality, and reduce costs. Our broad membership includes federal government agencies (including CMS and ASTP/ONC), state government agencies, patient advocate organizations, the leading health plans and health plan associations, the leading providers and provider associations, standards development organizations and the developer of operating rules, clearinghouses, and health IT vendors. With a focus on advancing standards for electronic administrative transactions, and promoting data privacy and security, WEDI has been instrumental in aligning the industry to harmonize administrative and clinical data.

WEDI supports and shares HHS's goals of leveraging Health IT's advanced capabilities and functions to decrease burden and streamline processes to improve the quality of care while minimizing administrative costs. We applaud CMS and ASTP/ONC's decision to release this RFI and solicit industry perspectives on these critical issues. Developing and implementing standards and processes that encourage the effective

and efficient exchange of health information will serve as an important catalyst for improving the nation's health care delivery system.

To aid us in developing our response to this RFI, WEDI conducted a Member Position Advisory (MPA) event on May 28, 2025. Through surveys, interviews, and live events, the MPA process is designed to solicit WEDI member input on topical issues, public and private sector proposals, or government regulations. More than 100 individuals participated in this MPA process to discuss this RFI, representing patient advocate organizations, health plans, providers, standards development organizations, clearinghouses, electronic health record (EHR) vendors, as well as consultants and other Health IT vendors.

General Comments and Recommendations

WEDI's mission and work are driven by easing administrative burden, putting patients at the center of their care, implementing consensus based, mature standards that support automation, and maintaining appropriate safeguards for privacy, security, and confidentiality. With its emphasis on patient empowerment and effective data exchange, WEDI supports the direction and purpose of this RFI and we applaud the work of CMS and ASTP/ONC to improve health IT and reduce administrative burden for all health care stakeholders.

WEDI's comments are based on key guiding principles that are integral and essential considerations of any regulatory action. Specifically, meeting the goals of the bipartisan 21st Century Cures Act and implementation of the CMS Interoperability and Prior Authorization Final Rule require that relevant stakeholders have ready access to several key capabilities and functions. Patients and providers must have access to the clinical data that leads to improved care delivery. New standards and new technologies offer the promise of more efficient data exchange and reduced administrative burden. As HHS explores opportunities to improve the health technology environment, it is important to design a transition that:

- Ensures the health information needs of the patient and their caregivers are at the center of the ecosystem.

- Promotes seamless, automated data exchange through mature, clear, and unambiguous standards that have been thoroughly tested and demonstrate meaningful return on investment (ROI).

- Integrates data exchange efficiently within the health plan, provider, and other end-users' workflows.

<u>Continued support for the CMS Interoperability and Prior Authorization Final Rule</u>
WEDI supports and shares CMS's goals of leveraging health IT's advanced capabilities and functions to decrease burden and streamline processes to improve the quality of care while minimizing administrative costs. We applaud CMS's decision to tackle the challenge of improving interoperability and the burden associated with prior authorization processes

and requirements. Encouraging industry stakeholders to adopt and use a uniform set of standards is an important step toward enabling the efficient exchange of health information and the automation of prior authorization workflows. Similarly, the payer-to-payer, provider access, and patient access Application Programming Interface (API) standards promise unprecedented opportunities for the exchange of health information.

We believe the access APIs will facilitate enhanced patient care coordination, close gaps in care, and more effectively support those health plans and providers in value-based care arrangements. Real-time electronic transactions also have the potential of reducing costs for payers and providers by reducing or eliminating manual processes (e.g., fax, phone, proprietary payer web portal) and decreasing human-to-human provider communications with health plans.

Efficient feedback loops

HHS should consider developing a process that could capture feedback from Health IT users and developers on the effectiveness of the functionality of Health IT. Most importantly, HHS should validate that required data elements and functionality incorporated into, for example, the certification process, are fully supported by the developer and effectively perform the role that they were intended. Capturing end user feedback, including patient and provider perspectives, could be accomplished, in part, by creating an anonymous survey that would encourage end users and developers to share their perspectives on the functionality of health IT, the certification process, and certified software itself. The goal of this process would be to capture real-world input to advise CMS and ASTP/ONC on future programs and requirements.

Real-world pilots

The health IT environment is constantly changing. CAQH CORE, Health Level Seven, National Council for Prescription Drug Programs, and X12 continue to develop new solutions and new implementation guides. While there is great promise with these new standards, there should be federal support for comprehensive pilot testing using real-world scenarios and conducted in multiple types of care settings. Additionally, these pilots should be conducted in a fully transparent manner with the results made public.

The value of piloting goes well beyond simply proving that a standardized approach works as intended. Piloting a new standard or approach can identify workflow issues that will either need to be corrected by revising the standard itself or addressed by stakeholders during implementation. Successful piloting of a new standard and/or workflow approach can serve to establish a clear return on investment-thus increasing support from plans and providers. This in turn can accelerate development of the supporting software. This momentum building within each stakeholder group is critical to avoid an overly protracted compliance glidepath.

Comprehensive regulatory roadmap

The transition to electronic prior authorization (ePA) and access APIs are only the beginning of the many Health IT requirements and implementations the industry is expected to face over the next few years. Uncertainty in terms of what requirements to meet and when to meet them can divert scarce resources and harm the industry's ability to meet these government mandates. The industry is also experiencing a significant

shortage in its heath IT workforce, especially those with API expertise. Conversely, regulatory certainty will permit impacted stakeholders to direct appropriate monetary and personnel resources. We urge CMS and ASTP/ONC to work with its federal partners to coordinate mandates and compliance dates and develop a regulatory roadmap that ensures a smooth implementation glidepath for all impacted organizations.

Establish an ongoing public advisory process.
In this ever-changing health IT environment, it will be critical for HHS to have ongoing industry input from the entities directly impacted by these policies. We recommend that CMS, ASTP/ONC and other appropriate HHS agencies leverage existing advisory bodies or establish and support a new public-private sector group convened under the Federal Advisory Committee Act (FACA). This FACA entity should be mandated to guide the Department as it furthers health IT and interoperability efforts and recommends additional automation opportunities.

Technology adoption assistance
Due to a lack of resources and technical expertise, small provider organizations historically have challenges optimizing Health IT to improve the quality of patient care they provide. This same need for technical assistance was an issue when the provider community was seeking to adopt Certified EHR Technology (CEHRT) and participate in the early days of the CMS Meaningful Use EHR Reporting Program.

HHS addressed this issue by deploying Regional Extension Centers (RECs) to offer technical assistance for solo and smaller provider practices and those who provide primary care services in public and critical access hospitals, community health centers, and other settings to implement and maintain EHRs. RECs established themselves as trusted advisors for these smaller care settings and facilitated the effective use of Health IT. The REC program was designed to leverage local expertise to provide practical, customized support to meet the needs of local healthcare providers. The REC core service areas included: (i) EHR implementation and project management; (ii) Health IT education and training; (iii) Vendor selection and financial consultation; (iv) Practice/workflow redesign; and (v) Privacy and security. Each one of these core service areas appear to mirror what small providers need to assist them implement CEHRT with ePA and generally for the transition to FHIR-based administrative solutions.

The most effective way to encourage providers to adopt ePA solutions is to establish a clear ROI related time saved by administrative and clinical staff. Absent that ROI, especially in times of economic uncertainty, providers will be very unlikely to invest resources in untried and untested technologies.

Specific Comments on the RFI

Patients and Digital Health

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

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

b. If you had a personal assistant to support your health needs, what are the top things you would ask them to help with? In your response, please consider tasks that could be supported or facilitated by software solutions in the future.

Applications (apps) or digital health products (products) that would be useful would include features that review the patient's data and offer personalized, specific suggestions for actions the patient could take based on their information. Those actions could be ones that would improve their medical condition or overall health needs. Patients have apps and products that collect various pieces of data or information. What is needed is an analysis of that data, whether in the standalone app or product or across disparate apps and products. The most useful outcome from that data and analysis would be suggestions and resources for what the patient could do next, such as contact their provider, take their medication, improve their behaviors, or continue their current actions. This enhanced functionality will require significant improvements in data flow.

App and product developers must work with patients to learn what features, data, and information will be most impactful to them and then work with providers and health plans on how to send and receive that data with the patient. Patients will have different wants and needs for apps and products. Developers should think more broadly about what to build for patients, keeping in mind how much can be included in one solution or how multiple solutions can be integrated. Different apps or products may be necessary for collecting and exchanging clinical information vs. administrative functions, e.g., scheduling appointments, paying a bill, or searching a provider directory. If the products are separate, optimally there should be a linkage that allows for cross-posting of data. Patients are looking for apps and products that give them a single dashboard of their health, medical, and wellness needs.

Patients would also like a point of contact within their provider network for who is managing their data. This most likely will be their primary care physician, care coordinator, or health navigator within their primary care physician's practice. It is important for patients to know their providers are informed of changes in their health based on data provided and to also know who oversees their data.

Another feature to consider for apps and products is allowing multiple users for a single solution. Users would be identified as patient, caregiver, and provider. This would give caregivers the ability to monitor their loved one's data and information. Having assigned users with logins and passwords will also offer transparency into who is viewing and creating content in the app or product.

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

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

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

c. Were there particular data types, such as x-rays or specific test results, that were unavailable?

What are the obstacles to accessing your own or your loved ones' complete health information electronically and using it for managing health conditions or finding the best care (for example, limitations in functionality, user friendliness, or access to basic technology infrastructure)?

For value-based care arrangements, it is necessary to integrate social care needs into apps and products that support overall health care and medical services. Connecting patients with community services, such as food banks, transportation, housing, is important for all patients, but in this case specifically for available waivers or other supplementary benefit enhancements. Apps or products that can help identify social services and coordinate these services would increase access to and use of them.

Access to x-rays, specific test results, or other data types not currently contained in the patient's portal is critical for patients to self-direct and manage their care. Diagnostic images are usually stored in a standalone system, which means they are often unavailable to share with another provider during referral or care coordination scenarios. It is burdensome for patients to have multiple apps and products, each with its own login and password, for each type of data needed to manage their care. The data needs to be in an interoperable form that can easily flow, with appropriate consent, to other providers.

PC-3. Are you aware of health management, care navigation, or personal health record apps that would be useful to Medicare beneficiaries and their caregivers?

Widely speaking, patients to date have not been active users of their data. Previous efforts with personal health records never gained staying power. Perhaps apps and newer products can offer data in a format and through a solution or tool that patients find easier to use and more meaningful in managing their health. With any technology, it is important to educate patients regarding the value, features, and positive outcomes health IT can have on their health journey.

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

a. What apps should exist but do not yet? Why do you believe they do not exist yet?

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

Most apps and products focus on capturing the data and, when possible, exchanging it with an authorized user. Providers and health plans would benefit from gathering information on the patient's experience with their health care encounters and treatment.

As discussed in PC-1, patients would like apps and products that include suggestions and resources that will drive them toward actions they should take.

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

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

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

CMS should consider options they have to incentivize patients to use apps and products, either directly through Medicare such as a discount on their Medicare premium, decrease in their co-insurance amount, rewards card, etc., or through incentivizing providers. Providers could facilitate app usage by their patients based on their knowledge of the patient and what will be most effective for them. Nominal incentives/education may push patients into using apps and products. Specific to value-based care, incentives for the patient could be included in the arrangement and would support closing gaps in care. Educating patients on the use of apps and products specific to their health condition and needs is also critical. The Center for Medicare and Medicaid Innovation could be an excellent platform to test various patient incentive options.

Another aspect of patients using apps and products is assurance that it is reliable and will meet their needs. The federal government should consider developing a process and system for rating or certifying apps and products. This initiative could be undertaken by HHS, the Federal Trade Commission (for apps that do not fall under the purview of the Food and Drug Administration), a combination of various federal agencies, or a public-private sector collaborative. The rating or certification should include an assessment of the functionality, usability, privacy, and security components.

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?

Patients need to have a level of assurance that the apps and products they are considering, at a minimum, have the functionality they need, are easy to use, integrate with other apps or products they use, and have privacy and security controls. Apps and products must also be something that the patient can make part of their daily life. Finally, they must be affordable and integrate seamlessly with their providers' and health plans' systems.

<u>The need for App security</u>
Some HIPAA covered entities (CEs), including health plans, physician practices and inpatient facilities have already built or have contracted with business associates to develop patient access APIs and apps and are actively promoting their use. Specifically,

these apps deployed by providers and health plans are typically covered under HIPAA and therefore the individual's accessing data have assurances that their information is being kept private and secure. We are concerned, however, regarding the lack of robust privacy standards applicable to the large percentage of third-party app developers not associated with CEs and therefore not covered under HIPAA and the fact that there currently is no federally recognized certification or accreditation for these apps. The potential exists for PHI gained via the apps to be inappropriately disclosed to the detriment of patients and their families. While we strongly support patient access to their PHI via apps, we assert that a national framework is required to ensure that health care data obtained by third-party apps is held to high privacy and security standards.

The protections afforded by HIPAA privacy and security have been a fixture in our health care system for more than two decades. These privacy and security rules lay out a framework to ensure that PHI will be kept secure, and patients rely on HIPAA to ensure that the confidentiality of their information is maintained. Organizations that are CEs under the law have a responsibility to take necessary steps to maintain the trust of individuals. However, these same individuals may not fully appreciate that individually identifiable health information collected outside of a HIPAA CE or under a business associate agreement (BAA) are not afforded HIPAA privacy and security protections.

We continue to be concerned that patients will not have adequate information to be educated consumers regarding third-party apps and may not fully comprehend that they are assuming the risk of the security practices implemented by their chosen app. Specifically, patients may not understand when their information is and is not protected by HIPAA.

We strongly support the September 15, 2021, FTC policy statement that health apps and connected devices that collect or use consumers' health information must comply with the Health Breach Notification Rule, which requires that they notify patients and others when their health data is breached. Recent evidence suggests that third-party apps in the health care environment are vulnerable to security issues. We note that the existing HIPAA Privacy Rule requires that, in many cases, patients be asked to sign a written authorization before their PHI may be shared with third parties. In requesting comments on whether CEs be required to educate or warn individuals that they are transmitting PHI to an entity that is not covered by these rules, we believe the Department is correctly assuming that there is potential danger in moving ePHI to third-party apps.

Again, while we are supportive of increasing data exchange for patients via third-party apps, there is a clear potential that using these apps could result in patients having their information inappropriately disclosed. We also assert that it is inappropriate to put the burden of warning the individual solely as the responsibility of the CE. CEs will typically not be experts on app data privacy and security protocols and will have little time to warn patients of the potential dangers associated with transmitting ePHI to third parties not covered by the HIPAA protections. Under current regulation, CEs are not permitted to require formal verification checks on individual third-party apps before allowing the application to connect to its API.

We believe that for health care data exchange to occur in an interoperable manner as called for under the 21st Century Cures legislation, there must be a consistent and high level of trust among all participants, including entities that are not legally a CE or bound by a BAA. The deployment of effective federal policies is critical to assist in facilitating this trust framework.

It is important to note that the CMS Blue Button 2.0 program itself recognizes the importance of third-party apps maintaining strict privacy protocols. For example, the Blue Button 2.0 Production Access Checklist includes an adherence to the Blue Button 2.0 API terms of service and general privacy guidelines. These guidelines include developers specifying: (i) data collection practices; (ii) the risks in their privacy policy; (iii) the company's data disclosure practice, including any use and sharing of de-identified, anonymized or pseudonymized data; (iv) the company's data access practice, including any use and sharing of de-identified, anonymized or pseudonymized data; (v) the company's security practice, including any use and sharing of de-identified, anonymized or pseudonymized data; and (vi) the company's retention/deletion practice, including any use and sharing of de-identified, anonymized or pseudonymized data. Collecting this information from developers will be a critical component of the agency's effort to protect the data of Medicare beneficiaries.

Further, the CMS Data at the Point of Care (DPC) API initiative is currently in a pilot phase in which a limited number of users can access Medicare Fee-For-Service claims data through the API once their solution has been approved for production. This pilot program promotes the industry standard FHIR, specifically the Bulk FHIR specification. We note that health IT implementers preparing to onboard the DPC production environment are required to provide one of the following CMS-accepted security certifications: (i) Office of the National Coordinator for Health Information Technology (ONC) Health IT Certification; (ii) HITRUST CSF Validated Assessment; (iii) HITRUST self-validation assessment (valid for one year from date of first implementation if currently pursuing the HITRUST validated assessment); Electronic Healthcare Network Accreditation Commission (EHNAC) Accreditation; System and Organization Controls (SOC) 2 type 1 certification (valid for one year from date of first implementation if currently pursuing type 2), or type 2 certified; and (v) International Organization for Standardization (ISO): 27001, 27017, or 27018 certified.

We offer the following recommendations that we believe will encourage organizations to take full advantage of electronic exchange and help patients reap the benefits of streamlined sharing of clinical data:

- Release additional guidance on the types of third-party app security and privacy verification that will be permitted and allow CEs themselves to undertake an appropriate level of review of a third-party app before permitting it to connect to their APIs.

- Require entities that are not HIPAA CEs or business associates to clearly stipulate to the individual the purposes for which they collect, use, and disclose identifiable health information and require that these individuals be given clear, succinct notice concerning the collection, use, disclosure, and protection of individually identifiable

health information that is not subject to HIPAA.

- Work with the private sector in the development of a privacy and security accreditation or certification framework for third-party apps seeking to connect to APIs of certified health IT. Once established, CEs should be permitted to limit the use of their APIs to third-party apps that have agreed to abide by the framework. Such a program would not only foster innovation but also establish improved assurance to patients of the security of their information.

- Apply similar security requirements in the private sector as CMS applies to its Blue Button 2.0 and DPC initiatives, requiring all third-party apps seeking to access PHI via provider or health plan APIs to prove adherence to a strict set of privacy and security guidelines or successfully complete a CMS-approved security certification.

- Partner with groups like WEDI and other professional associations in the development and deployment of education aimed at a wide range of consumers and CEs. Enhanced consumer and CE education will lead to significant improvement in the ability of the consumer and the CE to understand their rights and responsibilities under the law.

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)?

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

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?

As outlined above, the ability to link social care needs with community services is currently a gap in apps and products and would be beneficial for patients.

TEFCA

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?

WEDI applauds ASTP/ONC for developing the TEFCA framework and going live with the network. WEDI is strongly supportive of establishing a framework for the trusted exchange of electronic health information. TEFCA represents another phase of ONC's efforts to advance interoperability across the nation's health care system in support of the access, exchange, and use of electronic health information.

We also appreciate the agency proposing to improve the TEFCA infrastructure and add improved guardrails for Qualified Health Information Networks (QHINs). The current QHIN administrative process and onboarding methodology is focused very much on self-directed oversight and a less than optimally rigorous onboarding process. Needed improvements will shore up administrative processes and instill additional assurance for those seeking to leverage QHINs to exchange health data.

Patients want their necessary and appropriate information available at the time of their health service whether through an app or product they provide or through a behind-the-scenes data exchange methodology, such as one supported by TEFCA. Data exchange through TEFCA is still evolving and should be evaluated for its ability to meet patients' and providers' needs.

We strongly support ASTP/ONCs proposed modifications to QHIN administration. We urge the agency to finalize: (i) A more thorough verification process that includes background checks, validation of NPIs, and a rigorous review of organizational credentials; (ii) A more rapid decertification of QHINs found non-compliant or those engaged in fraudulent activity; and (iii) Enhanced monitoring of the use of QHIN and participant credentials. If fraudulent activity is detected, all parties must be contacted immediately, and appropriate actions taken to protect patient data and stop the continued use of those credentials.

ASTP/ONC has proposed adding a new part (172) to title 45 of the Code of Federal Regulations to implement certain provisions to establish the procedures governing QHIN Onboarding and Designation of QHINs, suspension, termination, and administrative appeals. We support these provisions as they will establish the qualifications necessary for an entity to receive and maintain designation as a QHIN capable of trusted exchange pursuant to TEFCA. We concur with the agency that these proposals, once adopted, will improve the reliability, privacy, security, and trust within the TEFCA environment. We believe that implementing these new requirements will instill additional public confidence in TEFCA and drive acceleration of TEFCA-led data exchange.

WEDI has the following comments and recommendations TEFCA and the draft QHIN framework:

- We recommend that participation in TEFCA continue to be voluntary.

- We strongly recommend ASTP/ONC actively work with the health plan community to ensure they are engaged and involved in TEFCA and are incentivized to participate fully in QHIN data exchange. To achieve that, we recommend ensuring that data fees do not serve to disincentivize plan participation. We also encourage the expansion of high-value use cases for health plans as a method to increase their participation.

- The HIPAA privacy framework has been a fixture in our health care system for more than two decades. Patients rely on HIPAA to ensure that the confidentiality of their information is maintained. Ensuring that TEFCA facilitates trust in the privacy and security of the information being exchanged as well as improved health outcomes for individuals will be critical to its success.

- For health care data exchange to happen in an interoperable manner as called for under the 21st Century Cures rules, there must be confidence that participants meet a minimum level of privacy and security. We recommend ASTP/ONC and the RCE explore requiring each participant within the exchange environment to complete an appropriate and independent third-party privacy and security accreditation.

- WEDI recommends ASTP/ ONC and the RCE move forward with support of FHIR-based standards as a more secure and scalable option for interoperable exchange of health information.

Leveraging new standards and technologies, including FHIR and HL7 Unified Data Access Profiles may offer a method to address current challenges and inability to scale solutions. We also note that the industry shift toward FHIR includes CMS and ONC regulatory requirements. As a result of these mandates, we are concerned that health plans and other impacted stakeholders have and will make a considerable financial and human investment in this new approach. Requiring an older unsupported standard (Integrating the Healthcare Enterprise) could force stakeholders to potentially incur the financial cost of supporting the two standards and necessitate the challenging task of identifying and hiring staff with expertise in the older standard. Overall, forcing stakeholders who otherwise would be interested in participating in the exchange framework to support multiple exchange standards could have the unintended consequence of limiting participation.

Further, there appears to be concern regarding the “maturity” level of FHIR for use in an exchange framework. As evidenced by the FHIR at Scale Taskforce (FAST), HL7 Da Vinci, and Argonaut initiatives, considerable progress has been made in developing FHIR-based exchange protocols. ASTP/ONC and the RCE should ensure that TEFCA and the ongoing work of ONC FAST, HL7, and the FHIR accelerators are aligned and leveraged. Impacted stakeholders must work together to create a unified, integrated and

agreed upon approach to move forward and establish a common exchange process implementation roadmap. We expect that avoiding duplication of effort and eliminating the requirement to support multiple standards will result in greater participation in the exchange network and this in turn will lead to a greater impact on patient care.

WEDI commends the work of the ASTP/ONC and the Sequoia Project as the Recognized Coordinating Entity (RCE) to advance the interoperability of electronic health information. The bipartisan 21st Century Cures Act pushed for interoperability to be a priority for the industry and TEFCA represents an important step towards achieving this goal. As ASTP/ONC further develops their approach to advancing interoperability, we encourage further collaboration with CMS, as well as industry stakeholders such as WEDI.

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?

b. What changes would you suggest?

c. Are there particular examples of high-performing HIE models that you believe should be propagated across markets?

d. 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.)?

Executing data sharing agreements has historically been the barrier to the exchange of patient data. TEFCA was created to address this issue and fill in any gaps between health information exchanges (HIE). Now with TEFCA, more organizations should be able to engage in data exchange, whether through an HIE or independently.

HIEs have the potential to play a central role in data exchange in regional communities where trust and support tend to be higher, facilitating more data exchanges. As patients and providers experience data exchange capabilities through HIEs, they will better understand the benefits. Patients are frustrated by the need to repeat their medical history and information to multiple providers throughout the care journeys. HIEs can solve this problem by allowing patient information from one provider to flow to another in the care team, with the patient's consent.

One consideration is to have HIEs function as a utility and manage them at the state level. This could bring commonality, capabilities, and expectations for the functionality related to interoperability, data exchange, and privacy and security.

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?

We recommend CMS provide education to the broad population of patients on what information blocking is and is not, and what the requirements are and are not. There is much confusion in the industry regarding what constitutes information blocking and what

are the exceptions to information sharing. In general, there continues to be confusion across the industry related to the HIPAA Privacy and Security Rules and what can and cannot be shared and under what circumstances. Additionally, patients often cannot distinguish whether their provider or the provider's certified health IT vendor is responsible for data blocking. Without clearly explaining to patients the roles and responsibilities of each actor—such as healthcare providers, certified health IT vendors, and Health Information Exchanges/Networks—complaints about information blocking may incorrectly identify the responsible party, wasting resources at ASTP/ONC and OIG. We believe providing specific (de-identified) examples of information blocking would be very beneficial to impacted stakeholders. CMS can leverage its existing communication channels for patients, providers, and others.

In addition, ASTP/ONC has proposed in the HTI-2 Notice of Proposed Rulemaking to revise the sub-exception to remove the existing limitation that applies the exception only to individual requested restrictions on EHI sharing that are permitted by other applicable law. We support the proposal to broaden the sub-exception's availability by removing its existing limitation to individual-requested restrictions on EHI sharing.

In addition, we concur with the agency that this proposal would lead to improved assurance for any actor who elects to honor an individual's request for restrictions on sharing of the individual's EHI that applying those restrictions will not be considered information blocking if the requirements of this sub-exception are satisfied. It is also expected to provide enhanced assurance for individuals that information blocking regulations support actors' choices to honor the individual's request and not share EHI when the individual asks that it not be shared. WEDI also supports the proposal to revise the sub-exception. We urge the agency to develop comprehensive guidance to ensure actors understand when and how the Privacy Sub-exception applies.

WEDI also support the addition of the "Requestor Preference" exception and urge the agency to finalize this new exception with one important modification. This exception would offer providers certainty that it would not be considered information blocking to adhere to a requestor's preferences for: limitations on the scope of EHI, the conditions under which EHI is made available to the requestor, and the timing of when EHI is made available to the requestor for access, exchange, or use.

We recognize the challenge of ensuring that while the patient still has full access to their health information when they need it, and in the format they request, there may be a desire on the part of the requestor to have information be first sent to and reviewed by their care professional. Actors should have the ability to discuss with their patients how they would prefer to receive health information such as laboratory or radiology results. Patients should have the right to dictate that these and other types of test results be sent directly to the care professional, who then can inform the patient, discuss the results, and plan the course of treatment.

We do recommend a change to the proposed exception. The proposal requires the patient to express their preference in writing, which we believe would be inappropriate. Patients trust their care professionals and should have the ability to communicate their preferences verbally during the consultation process. Adding yet another form for patients

to fill out and for providers to collect and store increases the administrative burden on both sides. As an alternative, we urge the agency to consider adding a field in the certification criteria that would permit the care professional to record patient preferences.

Digital Identity

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?

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

c. What are the potential downsides?

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

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

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

While the use of digital identity could be helpful for patient access to various apps and products, there will be limitations and challenges to its implementation. The process to obtain a digital identity can be cumbersome, as it includes completing an application, being vetted by the organization providing the digital identity, going in person to prove your identity, and paying an initial fee and the ongoing subscription cost. Not all patients will be able to or want to obtain a digital identity. Patient education will be needed on digital identity and credentials, including how to obtain one, how to manage it, how to link it to their apps and products, how to share it appropriately, and what to do if they have a problem with it.

It is unknown if the capabilities to support digital identities exist in current systems. Providers, health plans, and other users of digital identities will need to learn how to accept, store, protect, and share them. This will likely incur additional costs and could overwhelm smaller and rural organizations.

The proposal to implement digital identities raises the question about the never implemented, HIPAA-required national patient identifier. Development of the patient identifier was stopped following widespread concern about patient privacy and having a database with each individual and a linking identifier. While digital identity is not an all-encompassing database of individuals, there will be security concerns associated with it.

At this time, WEDI recommends additional work and an end-to-end pilot be done to evaluate the various aspects of the use of digital identities in health care. WEDI agrees with allowing the use of digital identities among willing trading partners and based on the receivers' (patient, provider, and health plan) ability. Digital identities should not be required until further study is done on their effectiveness in solving the problem for which they are being implemented.

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

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

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?

Demonstrating the use of digital identities with patients and other partners to successfully solve an existing workflow issue will encourage providers to adopt, accept, and share digital identities.

Providers rely heavily on their technology vendors to develop and implement solutions that address their needs. It is unknown at this time if the capabilities to support digital identities exist in electronic health records (EHR) and revenue cycle systems. Vendors will need to verify if a provider's current systems can accommodate digital identities. If not, vendors will need to build the solution and install it. Providers will need to learn how to accept, store, protect, and share them. All of this will come at a cost for the software installation or upgrade, training of staff, and ongoing digital identity service costs. Providers will want some assurance that the costs for accommodating digital identities will provide a return on investment and that there will be widespread usage by their patients and other partners.

In today's cyber environment, providers are often prime targets for cybersecurity and ransomware attacks because of the important and sensitive data contained in EHRs and revenue cycle systems. Storing digital identities and sharing them across users could make them more of a target for criminals wanting to steal this new data within their systems. This risk impacts patients whose digital identity would be compromised and overall patient care when services are stopped due to systems being offline. We recommend HHS evaluate the potential effect of digital identities on cybersecurity attacks and any preventive measures providers could employ to lessen their vulnerabilities.

Due to these various concerns, WEDI recommends that additional work be done by CMS, ASTP/ONC and other HHS agencies to develop a full understanding of the need, costs, and impact of implementing digital identities. WEDI agrees with allowing the use of digital identities among willing trading partners and based on the receivers' (patient, provider, and health plan) ability. Digital identities should not be required until further study is done on their effectiveness in solving the problem for which they are being implemented.

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?

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

c. What are the potential downsides?

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

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

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

There are several challenges for the implementation of digital identities for providers. The primary concern is how this project will fit within the timeline and budget of other projects currently underway to comply with multiple regulatory requirements. Providers have limited resources in terms of finances and staff to manage these many projects. Providers will need to have a clear understanding of how prioritizing an implementation of digital identities fits with the project plan of other requirements and the value it will bring to their organization.

As stated earlier, providers will need to have a full understanding of what problem is being solved with digital identity and whether the outcome will be achieved. Is this problem large enough and will the solution resolve it in a manner that will make it worth the costs of implementing and maintaining it.

Other barriers include available technology, costs, resources, and usage by patients. Providers rely heavily on their IT vendors to provide these types of solutions, and this comes at a cost. Smaller and rural providers are currently under immense financial pressure and do not have readily available resources for a project of this scope. An outstanding question is also whether patients will obtain digital identities and then want to use them in their health care interactions. Providers will not want to invest in this technology if it is not widely used by their patients and other partners.

Again, WEDI recommends that additional work be done by CMS and other HHS agencies to develop a full understanding of the need, costs, and impact of implementing digital identities. WEDI supports allowing the use of digital identities, but they should not be required until there is a better understanding of their effectiveness.

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?

Providers will want to see a proven use case for how digital identities will enhance identity management while reducing burden and cost. HIEs are currently managing their patient matching capabilities using algorithms and not digital identifiers. Additional information is needed to understand the current need and how digital identities will address it.

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?

As we have stated, there are several challenges for the implementation of digital identities for payers. Payers, like providers, will want to understand how this project will fit within the timeline and budget of other projects currently underway to comply with multiple regulatory requirements. Payers will want a clear understanding of how

prioritizing implementation of a digital identity solution fit with the project plan of other requirements and the value it will bring to their organization.

Payers will also want a full understanding of what problem is being solved with digital identity and whether the outcome will be achieved. They will want a proven use case for how digital identities will enhance identity management while reducing burden and cost.

CMS and other HHS agencies should develop a full understanding of the need, costs, and impact of implementing digital identities. WEDI supports allowing the use of digital identities, but they should not be required until there is a better understanding of their effectiveness.

TD-3. Regarding digital identity implementation:

a. What are the challenges and benefits?

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?

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

The challenges for technology vendors, data providers, and networks (collectively referred to as “vendors” hereafter) related to implementing digital identity specifications are similar to those of providers and payers. Vendors will want to understand how this project will fit within the timeline and budget of other projects currently underway that will support their customers’ requirements and needs. Vendors will want a clear understanding of how prioritizing the implementation of digital identity will benefit their customers.

Providers are currently prime targets for cybersecurity and ransomware attacks because of the rich source of data contained in EHRs and revenue cycle systems. Vendors will need to determine if there are any additional system capabilities that can be deployed to better safeguard the digital identity data. It is likely that providers having this data in their systems will make them more of a target for criminals. CMS should complete a thorough evaluation of the potential effect of digital identity on cybersecurity attacks and any preventive measures providers could employ to lessen their vulnerabilities.

WEDI recommends that additional work be done by CMS and other HHS agencies to develop a full understanding of the need, costs, and impact of implementing digital identities. WEDI supports allowing the use of digital identities, but they should not be required until there is a better understanding of their effectiveness.

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

As with other stakeholders, value-based care organizations need a better understanding of what problem is being solved with digital identity and whether the outcome will be achieved. They will want to see a proven use case for how digital identity will enhance identity management while reducing burden and cost. Additional information is needed to understand the current need and how digital identity will address it.

As the Department seeks to support the transition to value-based care, WEDI recommends that additional work be done by CMS and other HHS agencies to develop a full understanding of the need, costs, and impact of implementing digital identities. WEDI supports allowing the use of digital identities, but they should not be required until there is a better understanding of their effectiveness.

USCDI

TD–7. To what degree has USCDI improved interoperability and exchange and what are its limitations?
a. Does it contain the full extent of data elements you need?
b. If not, is it because of limitations in the definition of the USCDI format or the way it is utilized?
c. If so, would adding more data elements to USCDI add value or create scoping challenges? How could such challenges be addressed?

The United States Core Data for Interoperability (USCDI) standard is a baseline set of data that can be commonly exchanged across care settings for a wide range of use cases. While v3 is currently required as part of the ASTP/ONC Health IT Certification Program criteria, v4 has been proposed. We support requiring USCDI v4 as part of the Health IT Certification Program.

We note that there was some support among WEDI members for adopting USCDI v5, as ASTP/ONC approved USCDI v5 earlier, the majority supported establishing USCDI v4 as the baseline standard for data elements to be collected under the Certification Program, a January 1, 2028, start date for v4, and supported establishing an expiration date of January 1, 2028, for USCDI v3 for purposes of the Certification Program.

Certification

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

We are strongly supportive of ASTP/ONC including ePA into the provider ONC Health IT Certification Program. Publication of the landmark CMS Interoperability and Prior Authorization Final Rule earlier this year established an API-based communication protocol between the provider and the health plan that we believe has the potential to significantly streamline the prior authorization process. As software developers supporting providers are not covered entities under HIPAA, CMS requires that providers participating in one of the Medicare EHR incentive programs attest to completing at least one electronic prior authorization utilizing an API.

By creating an ePA certification component, ASTP/ONC has the potential of streamlining the prior authorization process and decreasing administrative burden and cost for both health plans and providers by: (i) Reducing the volume of calls between providers and health plans simply to establish whether a prior authorization is required; (ii) Clarifying the clinical documentation required to support a prior authorization; (iii) Eliminating lost health plan requests for additional documentation and provider responses; (iv) Reducing the

cost associated with staff manual collection of supporting documentation; (v) Decreasing plan documentation requests as there would be improved predictability of plan content needs (i.e., plans could be specific in what they required to render an authorization decision), thus eliminating the time consuming "back and forth" that currently exists in the system; and (vi) Reducing pended decisions, administrative appeals, and costly peer-to-peer discussions, resulting in increased adherence to health plan policy and faster treatment approvals.

Establish effective certification timing

The expansion of the ASTP/ONC certification program to incorporate access and prior authorization APIs will be important steps on the road to full industry adoption of this standard. We continue to be concerned that if the appropriate certification timing is not developed, it could result in needless costs, delays in benefits for health plans, providers, and patients, as well as unnecessary stakeholder burdens. We recommend ASTP/ONC work closely with CMS to ensure the appropriate implementation glidepath is established. We note that delays in implementing the ePA certification could create greater inertia, if not resistance, in the provider marketplace and create confusion for plans seeking to take advantage of automating prior authorization. WEDI also recommends CMS explore phasing in the Da Vinci API requirements, with Coverage Requirements Discovery (CRD) being considered for the initial implementation.

We believe the optimum glidepath would have the ONC provider Health IT Certification Program go live prior to the January 1, 2027 compliance date established in the CMS Interoperability and Prior Authorization Final Rule for the API requirements. To advance provider implementation efforts, the compliance date for the Health IT Certification Program ePA certification requirements should occur optimally no less than six months prior to the January 1, 2027, date providers and plans will begin exchanging data using these new standards.

Intersection with the X12 278 transaction

It is uncertain how providers and health plans will continue leveraging the HIPAA mandated X12 Health Care Services Review and Response transaction (278). According to the 2024 CAQH Index Report, while industry adoption of the X12 278 remains low at 35%, it has gone up from just 13% in 2019.

Further, while we appreciate the release on February 23, 2024, of the CMS X12 278 enforcement discretion for all HIPAA covered entities, we remain concerned that this discretion could be sunsetted at any time. Requiring the inclusion of the X12 278 transaction as part of the API process would result in needless burden and cost for both providers and health plans. With that in mind, we urge CMS to finalize the HIPAA exception regarding use of the X12 278 transaction in the PA process when stakeholders conduct electronic PA with APIs.

Should the ONC Health IT Certification Program only support FHIR-based APIs, it is unsure how EHRs will effectively conduct prior authorizations with providers and health plans that continue to use the X12 278 standard. We anticipate there will be a significant length of time past the January 1, 2027 ePA compliance date when providers will use the X12 278 to conduct prior authorization transactions with their health plan partners. We

urge ASTP/ONC to work with CMS to address how the use of the FHIR standard will interact with the long-term use of the HIPAA-mandated X12 278.

Health plan certification

While we appreciate ASTP/ONC proposal to stand up a certification program for those Health IT developers that support health plan efforts to meet the API requirements in the CMS Interoperability and Prior Authorization Final Rule, we recommend an alternative approach.

HIPAA designated providers, health plans, and clearinghouses as "covered entities" under the law but excluded software developers. Thus, the certification program for Health IT software developers was developed to serve as a catalyst for providers to adopt EHR technology that met the requirements of the CMS inpatient and outpatient EHR incentive programs. Participation by providers in these CMS incentive programs continues to be voluntary, although there are significant financial incentives and disincentives associated with the program.

Under the CMS Interoperability and Prior Authorization Final Rule, providers are not required to comply with the prior authorization APIs, although incorporation of the APIs is included in the CY 2027 performance period/2029 MIPS payment year for the Medicare Promoting Interoperability Program. Incorporating prior authorization APIs in an EHR certification is appropriate as it, again, will serve as a catalyst for providers to take advantage of this administrative simplification opportunity.

The 2024 CMS Interoperability and Prior Authorization Final Rule applies only to Medicare Advantage plans, Medicaid and CHIP managed care plans, state Medicaid and CHIP Fee for Service (FFS) programs, and Qualified issuers on the federally facilitated exchanges (FFEs). The health plans impacted by the CMS Interoperability and Prior Authorization Final Rule are legally required to comply with the prior authorization APIs included in the regulation. Offering a voluntary prior authorization API certification would be redundant and we do not believe a significant number of impacted health plans or plans not mandated in the Final Rule to support the prior authorization APIs, would incur the expense of seeking certification. Further, those providers seeking to connect via APIs with impacted health plans after January 1, 2027, who found that the health plan was unable to support the prior authorization APIs, will have the ability lodge a formal complaint against the health plan directly to CMS.

Deploying APIs in support of prior authorization is new to the health care industry. As an alternative to offering a voluntary Health IT Certification Program for developers serving the health plan market, we recommend an expansion of the HL7 Inferno testing platform that would allow both health plans and providers to test their individual ability to support the APIs. Inferno, as an open-source tool, creates, executes, and shares automated conformance tests for the FHIR® Standard. Inferno on HealthIT.gov hosts tests created with Inferno, but Inferno is also designed to allow the creation and hosting of individual tests. ASTP/ONC should also explore the option of expanding the platform to include testing end-to-end business processes.

With augmented support from ASTP/ONC, this expanded Inferno platform could offer all testing entities (health plans, providers, and their supporting vendors) both an opportunity to test systems and processes, and the ability to publicly report successful testing. We believe that public reporting of successful tests would incentivize other entities to conduct testing and report success.

WEDI makes the following additional certification recommendations:

- **Fully harmonize the certification criteria to the CMS Interoperability and Prior Authorization Final Rule requirements**. It is imperative that the API requirements of the ONC Health IT Certification Program be harmonized with the requirements mandated by the CMS Interoperability and Prior Authorization Final Rule. Deviation from these requirements will lead to industry confusion and the potential for less than optimum industry adoption of this new technology.

- **Develop an ePA module certification program to support all providers.** There are a significant number of provider types that traditionally do not participate in one of the CMS EHR incentive programs. These include pediatricians, dentists, physical therapists, and others. Many of these providers use EHR technology that is specifically designed to meet the needs of that specialty and does not require all the functionality that is included in the ONC certification criteria. Therefore, in many cases these "specialty" software products will not be certified under the ONC Health IT Certification Program. To allow these specialty vendors to offer products that conform to the ONC ePA requirements and take advantage of the API automation opportunities, we encourage ASTP/ONC to work with these specialties and design an ePA specific certification approach that meets their needs and facilitates support of the CMS Interoperability and Prior Authorization Final Rule API requirements.

  Similarly, we encourage ASTP/ONC to develop a module approach that conforms to the ONC ePA requirements to support self-developed EHR software. These self-developed EHRs often meet the needs of specific providers-some of whom may not require the complete functionality required from the full ONC certification. Allowing these products to certify to the ePA requirements in the CMS Interoperability and Prior Authorization Final Rule will allow these providers to take full advantage of the ePA API automation opportunities.

- **Integrate real-time solutions into the certification requirements when available.** The 2020 ONC report "Strategy on Reducing Regulatory and Administrative Burden Relating to the Use of Health IT and EHRs," includes recommendations for improving prior authorization processes. On page 18 of the report, ONC signaled its clear support for real-time ePA transactions when it makes the following recommendation: "Support automation of ordering and prior authorization processes for medical services and equipment through adoption of standardized templates, data elements, and real-time standards-based electronic transactions between providers, suppliers and plans."

  Real-time ePA transactions such as the CRD have the potential of reducing cost

for health plans and providers by eliminating manual (e.g., fax, phone, and proprietary plan web portal) communications from the provider to the plan. These real-time CRD decisions on whether a medical service requires a prior authorization is an important step toward reducing administrative burden for both plans and providers.

Requiring adherence to finalized HL7 Da Vinci Implementation Guide that includes a real-time response (as defined in the Implementation Guide) from the health plan to the provider's use of the CRD API should be a goal of the certification program. It is important to note that in the CMS Interoperability and Prior Authorization Final Rule, the agency recommends adherence to the HL7 Da Vinci ePA Implementation Guides but does not require adherence. We are hopeful that once providers have the capability to initiate real-time CRD, impacted and non-impacted providers will be incentivized to purchase the technology and health plans incentivized to support this approach. We believe the eventual move to real-time CRD will decrease provider use of manual approaches to establish whether or not a service requires authorization from a health plan.

- **Work with CMS to incorporate drug PA APIs into the certification criteria.** We note that although prior authorizations for medications was not required in the CMS Interoperability and Prior Authorization Final Rule, it was included in the Spring 2024 Unified Agenda under the title "Interoperability Standards and Prior Authorization for Drugs (CMS-0062)." The Unified Agenda states "*This rule CMS would propose new requirements for Medicare Advantage (MA) organizations and Qualified Health Plans (QHPs) offered on the Federally-facilitated Exchanges (FFEs) to streamline processes for the prior authorization for certain drugs. We are developing this rule, in part, based on the significant number of public commenters who responded to the CMS Interoperability and Prior Authorization proposed rule (87 FR 76238) urging CMS to expand the proposed prior authorization policies to include drugs. Increasing physician access to these high-value functionalities will address well-known transparency issues and administrative burdens related to drug prescribing and PA*." Including drugs covered under a patient's medical benefit plan as part of the prior authorization APIs would significantly improve the usability of the APIs, would decrease administrative costs for health plans and providers, incentivize those health plans and providers not impacted by the Final Rule to adopt the technology, and improve the care delivery process for patients.

- **Support for eRx and RTBT.** We strongly support the inclusion into the base EHR certification criteria of both NCPDP standards for electronic prescribing (eRx) and the real-time prescription benefit (RTPB). We urge ASPT/ONC to align with the CMS final rule requiring use of the NCPDP RTPB Standard Version 13. According to NCPDP, RTPB was developed to harmonize, as much as possible, with the NCPDP SCRIPT Standard and the NCPDP Telecommunication Standard. It supports information related to products and services covered under the pharmacy benefit and includes medications, vaccines, supplies/devices, and prescription digital therapeutics.

Both the updated eRx standard and RTPB standards will add significant value to the entire care delivery process. With eRx, there is decreased administrative burden for ordering clinicians and pharmacists, and improved medication adherence with patients. RTPB allows providers to receive accurate information regarding whether an ordered prescription is in the patient's health plan formulary, whether the prescription requires prior authorization, what the patient out-of-pocket costs will be, and potentially any appropriate therapeutic alternatives. This benefits the health plan by reducing the number of prior authorization requests from the provider and having the RTPB system steer the provider toward an in-formulary, lower cost option. For the care professional, these automated approaches can significantly decrease administrative costs and improve patient medication adherence.

Patients finding out once they arrive at the pharmacy that their prescription is prohibitively expensive may not fill the prescription and therefore not receive the expected benefits. Many may be forced to contact the care professional for additional consultations, adding burden to themselves and their care professional. With the RTPB system in place, patients are more likely to receive the appropriate prescription, receive it faster, and at a lower cost.

Certification and value-based care

Value-based care serves as a key foundation for CMS' strategy to incentivize improvements in health outcomes rather than increases in the volume of services. We concur that the deployment of effective technology is critical to this transformation. It is clear there are significant opportunities to better align technology requirements with the needs of providers participating in Alternative Payment Models (APMs) and other value-based care programs. It is critical to deploy a coordinated federal strategy that aligns positive incentives, standards, and support mechanisms to accelerate digital transformation in value-based care. Among other areas of inquiry, CMS and ASTP/ONC request input on requirements for the use of CEHRT, and how such requirements can enable value-based care and meet statutory requirements while meeting other program objectives, such as reducing provider burden, to better support value-based care adoption among providers, and subsequently improve patient choice and competition in the healthcare marketplace.

Bulk FHIR

TD–15. Regarding bulk FHIR APIs: a. How would increased use of bulk FHIR improve use cases and data flow?

Bulk FHIR offers significant promise of effective data exchange with a number of use cases. We believe bulk FHIR-based exchange can augment the "one-off" queries that are more common today. Providers seeking data downloads for a group of patients would greatly benefit by having bulk capability. Similarly, both health plans and providers in value-based care arrangements could effectively leverage bulk FHIR to exchange patient information. Public health and quality reporting are also potential use cases.

There are challenges associated with bulk FHIR, including potential costs. Also, it will be important to deploy appropriate guardrails around who can pull and consume bulk data. We also recognize that data is retrieved based on resource type and then must be stitched back together to put the pieces together. This process can be very difficult, especially for new users. Overall, we encourage the development of bulk FHIR as it could address many provider and health plan data needs but at the same time we encourage the development of appropriate guardrails. We also recommend CMS and ASTP/ONC ensure that the bulk-FHIR standard is well tested prior to it being required.

Price Transparency

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?

WEDI fully supports consumers having timely and accurate pricing information to improve health care decision making. It is, however, imperative that an appropriate balance be struck between the value for consumers and the burden on stakeholders to produce and maintain this information.

While Medicare and other government health plans are not subject to the No Surprises Act (NSA), requirements of the law have introduced the potential for significant burdens on providers who care for Medicare beneficiaries and health plans that administer benefits for them. WEDI has submitted several letters to HHS and CMS making recommendations for alternative approaches to meeting the requirements established in the NSA.

GFE and AEOB

Since passage of the landmark legislation the industry has had time to closely evaluate the new workflows, processes, and functions that would need to be implemented to meet the legislative requirements for generating Good Faith Estimates (GFE) for both insured and uninsured patients and Advanced Explanation of Benefits (AEOB) for insured patients. Currently, there are no existing data exchange standards that fulfill the operational requirements of the GFE, the AEOB, or the “convening provider” provisions of the law. To meet the intent of the law, WEDI recommends that CMS consider the objectives of the GFE and AEOB requirements, to provide consumers with timely and accurate cost information, and identify alternative methods to achieve these goals.

For insured consumers, CMS should explore the use of online price estimator tools on publicly accessible websites where the consumer has immediate access to a broad range of accurate medical service pricing information. WEDI also urges a public-private sector collaboration to develop and test NSA data exchange standards and workflow processes. Finally, WEDI strongly recommends that CMS exercise its discretion and not enforce any

NSA data exchange requirements until appropriate transactions have been identified, fully tested, and determined to function correctly.

Further, WEDI urges CMS to develop and disseminate educational materials to assist consumers in better understanding their rights under the NSA and how they can best use cost, quality, and other data to access affordable quality care. WEDI, with its multistakeholder membership, is ready and willing to collaborate with CMS on this effort.

National Health Care Directory

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

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?

WEDI applauds and supports the efforts of CMS to explore innovative approaches to collecting provider data and improving the accuracy of that information. WEDI shares the Agency's commitment to facilitating interoperability, reducing administrative burden, and enhancing the ability of consumers to access accurate and actionable data. As the Department explores various options for developing a National Health Care Directory (NHCD), we urge the process to be a public-private sector collaboration. As the collective voice of the health care industry on health IT issues, we are pleased to continue our important partnership with CMS as you and your colleagues develop regulations, industry guidance, and educational programming on the NHCD and other related initiatives.

Creating and maintaining an accurate directory of hundreds and thousands of physicians and other providers and ensuring that it is up to date is a challenging task. Government and commercial health plans rely on real-time, accurate provider data to deliver effective and high-quality member experiences and comply with applicable regulations. The No Surprises Act, included in the Consolidated Appropriations Act of 2021, recognizes the challenges consumers face in accessing accurate data by placing new requirements on providers to regularly report information and health plans to maintain accurate directories.

As we will outline in our comments, while there are many challenges that must be overcome, if the NHCD is developed in such a way that the nation's providers accurately report their data and federal and commercial health plans populate their directories with this information, provider administrative burden and industry cost will be significantly reduced.

The research studies conducted by CMS over the past few years identified a consistent level of inaccurate information and opportunities for improvement in provider directory maintenance. CMS released the results of its third round of annual review of the Medicare Advantage Organizations (MAOs) provider directories completed its third round of Medicare Advantage (MA) online provider directory reviews between November 2017 and July 2018. The review examined the accuracy of 108 providers and their listed locations selected from the online directories of 52 Medicare Advantage Organizations (MAOs),

approximately one-third of MAOs, for a total of 5,602 providers reviewed at 10,504 locations. The review found that 48.74% of the provider directory locations listed had at least one inaccuracy. The types of inaccuracies included: (i) The provider was not at the location listed; (ii) The phone number was incorrect; or (iii) The provider was not accepting new patients when the directory indicated they were.

This CMS research suggests that the current directory environment has resulted in a unacceptably high inaccuracy rate. Why has it proven so difficult to report and present provider data? Provider information is complex and incorporates myriad data elements such as contracting relationships, network tiers, and multiple provider locations. Making it even more challenging, the data are dynamic and constantly changing such as the requirement for directories to indicate which providers are accepting new patients. Providers, especially large group practices with potentially hundreds of practitioners, face significant challenges keeping information current. As a result, health plans encounter difficulties ensuring that data is up to date. Further, with no standard data set and no standard interface or reporting approach, providers are required to submit often different information through multiple interfaces resulting in considerable administrative burden.

As envisioned, a NHCD could reduce the overall burden of keeping health care directory data up-to-date and accurate. At a minimum, harmonizing the provider information requirements for the National Plan and Provider Enumeration System (NPPES) and the Medicare Provider Enrollment, Chain, and Ownership System (PECOS), as well as for other federal programs, would reduce provider reporting burden significantly. We concur with CMS that providers and their staff would be more likely to keep a single repository updated and verify it more frequently. However, to make the greatest impact, providers of all types must be incentivized to participate, the data must be accurate and verified, and commercial health plans must be incentivized to leverage this data for their own directories. We also encourage CMS to work with the industry to understand and solve the root causes that lead to directory inaccuracies and burden.

The development of an NHCD presents a unique opportunity for the federal government to collect and disseminate information that would directly assist underserved and disadvantaged communities. Collecting information on such entities as food banks, mental health services, transportation assistance programs, and other social services and then making that information available to consumers, organizations that assist underserved and disadvantaged, providers, health plans, and API developers would be extremely beneficial.

There are multiple potential stakeholder types that would engage with the NHCD, with each requiring a unique approach to incentivizing participation:

- **Providers/health systems**: One of the most effective motivations for providers to participate in the NHCD will be the opportunity to significantly reduce the number of entities they are required to report data to. Requiring providers currently participating in Medicare and Medicaid programs to enter their data into the NHCD will be one potential way to jumpstart the directory.

  Creating a streamlined process and standardized set of data will greatly reduce the

time and effort it takes to complete the reporting process and will encourage providers to participate. Communicating the opportunity for providers themselves to have access to accurate information for referrals and other purposes could serve as an incentive to participate. Reminding providers that timely reporting of accurate data will also benefit them as consumers will be accessing this information as they select services and locations. Any new directory effort should not create additional requirements but rather streamline the submission and updating of data.

Finally, we urge the deployment of a modern computing approach (perhaps block chain) to collect not only information CMS needs but also what the private sector needs in a way that reduces how many questions providers are asked (or how many times they have to make updates).

- **Health Plans**: Health plans (and programs) under the Agency's direct regulatory control can be the first to participate in the NHCD. Requiring NHCD participation from these entities will be an important step in creating legitimacy in the NHCD and would serve as an additional incentive for providers to report their data. CMS should also explore opportunities to incentivize Medicare Advantage plans to participate in the NHCD.

  Commercial health plans could have very specific provider information requirements such as identifying exactly which location a provider is offering specific services covered under a benefit plan. Even if a health plan was to leverage the NHCD to populate its directory, the plan may still be required to reach out to their providers to obtain and then verify additional information. Understanding these challenges, we believe that for commercial health plans to utilize the NHCD there must be a clear return on investment (ROI). To establish this ROI, we recommend CMS work with one or more commercial health plans to pilot test use of the NHCD data as a replacement to its proprietary database. The results from this pilot could serve as an incentive for other commercial health plans to use the NHCD for their directories.

- **Public health entities**: The incentive for public health entities to participate in the NHCD is clear-the receipt of more timely and accurate data. To encourage those public health entities that are not under the regulatory control of CMS, value of the NHCD and the benefits afforded to them by accessing accurate NHCD must be clearly communicated.

- **Vendors and clearinghouses**. Vendors, including API developers and those assisting providers and health plans meet their directory requirements, as well as clearinghouses that operate in the directory space should be included in any NHCD outreach efforts. Although they will have a commercial interest in the NHCD, they may still require technical information on how to both report data on behalf of their clients and leverage NHCD data for their products.

Once operational, the NHCD should be evaluated on a regular basis for its impact on targeted stakeholders. For example, consumers, specifically underserved and

disadvantaged populations, should be regularly surveyed for their knowledge of and use of the NHCD. Similarly, providers should be surveyed regularly for their knowledge of the NHCD, level of burden providers face in entering, updating, and accessing their information. Providers should be asked to rate the level of burden required to enter NHCD data compared to the burden required to enter commercial health plan directory data. Importantly, it will be critical to determine the ROI for health plans to access and use provider directory information. Should it prove cost efficient for a health plan to leverage NHCD data to populate its provider directories compared to its current approach, that information could incentivize other health plans to take advantage of the NHCD.

Centralization and standardization of provider data collection and effective dissemination of that data has the potential of adding utility for all stakeholders seeking to access provider information and reducing burden for those reporting the data. As we have discussed, to achieve the benefits outlined in this RFI it will be critical to appropriately incentivize those individuals and organizations that the Agency is encouraging or requiring to report data.

Providers included in the NHCD

To ensure the maximum utility of the NHCD it will be important to include as many providers and organization types as possible. Allied health professionals, post-acute care providers, dentists, emergency medical services, nurse practitioners, physician assistants, certified nurse midwives, providers of dental, vision, and hearing care, behavioral health providers (psychiatrists, clinical psychologists, licensed professional counselors, and licensed clinical social workers are all potential billing providers and should be included in the NHCD. However, there needs to be considerations for different provider types. It is unlikely that the data required for one type of provider is going to align or be appropriate to all others. We urge the Agency to work with provider professional associations to determine the minimum data requirements for each provider type.

Further, including organizations such as pharmacies, public health entities, community organizations, and nursing facilities would also be valuable both for consumers of health care and providers of health care. It would also be helpful to include in the NHCD suppliers of health care such as durable medical equipment. Finally, as the industry adopts the Trusted Exchange Framework and Common Agreement and associated Qualified Health Information Networks, it would be valuable to both consumers and providers to include these and other types of health information networks in the NHCD.

We also urge CMS to explore including “atypical providers” in the NHCD. These would be organizations who, for example, build wheelchair ramps for consumers, beneficiaries, and others. We note that these atypical providers as well as allied providers may have little experience with reporting to centralized data repositories and CMS may need to conduct outreach to these communities to educate them on the NHCD.

While adding these allied and affiliated provider entities will be beneficial, we recommend that CMS initially focus on capturing information from the core set of providers, with outreach to these allied and affiliated providers conducted in a later stage.

Including additional information

We believe it would be beneficial to consumers to include in the NHCD provider languages spoken other than English, specific office accessibility features for patients with disabilities and/or limited mobility, accessible examination or medical diagnostic equipment. We also note that consumers may find it helpful to know if staff at provider offices support languages other than English.

We do recommend CMS explore the option of including provider telehealth capabilities in the NHCD. For many consumers, knowing that the provider presents the option of a virtual visit could be an extremely important factor for consumers that may face transportation challenges or live a long distance from a provider office. We do recognize, however, that establishing a provider's ability to support telehealth will have its challenges-establishing the type of technology supported, if telehealth be supported at each of the provider's locations, what specific services are supported by telehealth, and whether a patient's health benefits include telehealth services.

FHIR Endpoints

With the large number of health plans and health plan products in the marketplace, a critical element for API success will be the ability of providers to quickly and accurately identity a specific FHIR endpoint. We urge CMS ASTP/ONC to work with industry to include endpoints in a NHSD or stand up a FHIR Endpoint Directory that is freely accessible by all health plans and providers.

Potential use of an NHCD

There are numerous potential use cases for the NHCD, including providers exchanging data to streamline the referral process, to promote care management programs, to support value-based care arrangements, and improve public health reporting. Currently, it is common that providers share patient data manually, either by printing the information and having the patient hand deliver it, using postal mail, or faxing the information. Having access to information such as Direct email addresses and FHIR-end points could facilitate automated data exchange.

The COVID-19 pandemic highlighted a need for public health systems to be better connected to providers and with each other. A robust NHCD that includes public health entities has the potential of offering a centralized approach to public health reporting for providers-thus decreasing the administrative burden associated with submitting data. We recommend CMS work with provider groups and public health entities to develop a reporting process that best meets the needs of each stakeholder group. In addition, centralizing the data collection ensures that CMS, in concert with other federal and state public health authorities, will be in a better position to analyze the data received and take appropriate actions based on that data.

Health plan access

For the NHCD to significantly decrease the burden associated with provider reporting it will be critical for commercial health plans to have access the NHCD to populate their directories. To achieve this goal commercial health must be incentivized to use the NHCD for at least some of their data requirements. We recommend CMS explore health plan incentive options that would include: (i) Creating a safe harbor from any directory

accuracy-related enforcement action for any plan that utilizes NHCD data to populate their directories; (ii) Establishing a clear ROI for a health plans to leverage NHCD data by conducting a pilot and publicly sharing the results; and (iii) Establishing that the quality and validity of the provider information captured in the NHCD is as good or better than the plan's current directory.

Addressing waste, fraud, and abuse

A potential use case of the NHCD to help prevent fraud, waste, abuse, and improper payments would be to more accurately identify unauthorized individuals and entities before they are enrolled into government or commercial health plans. Understanding this, if the NHCD is to combat fraud, waste, abuse, and improper payments, it will be critical to institute an effective verification process to minimize the chance that an unauthorized individual or entity is accepted into the directory.

Cybersecurity

In terms of privacy breaches, a centralized database as opposed to multiple proprietary provider databases of provider information could potentially decrease the likelihood of a breach, should the centralized database have appropriate security measures in place. We recommend that CMS deploy comprehensive and sophisticated cybersecurity policies and technologies to minimize the chance that the NHCD will experience a data breach.

Additional NHCD use cases

Additional use cases, such as licensing, certification, or credentialing should not be considered in the initial phase of the NHCD development. CMS should also review current industry solutions in these use case areas and explore opportunities to align the NHCD with these efforts. In addition, we believe it may be helpful to identify providers and health systems who participate in value-based care arrangements/alternative payment models. As well, identifying providers and health systems that are conducting clinical trials and/or hosting a training or residency program may also be beneficial. However, these may be data points to be captured in later phases of NHCD development.

Frequency and method of data updates

The general consensus from the WEDI membership was that providers should be required to update the majority of their NHCD information no more frequently than on a quarterly basis. However, certain data may require more timely updates. For example, when a provider leaves a location, when a provider joins an organization, and changes to locations where providers practice should be updated more frequently. Also, licensure and credentialing information that has changed should be updated on a more frequent basis. We also asked our members what the cadence should be for CMS to update the NHCD data requirements (based on new legislative, regulatory and other requirements). The consensus was that CMS should update the NHCD reporting requirements on not less than a yearly basis. We also recommend CMS permit multiple reporting approaches. For example, the NHCD should accommodate batch uploads, submissions from third-party vendors and clearinghouses, and receive data feeds from verified sources that already collect provider information.

We also note that an alternative to a "centralized data hub" is a decentralized approach where the NHCD functions as a network of public and private sector entities including

providers, health plans, public health agencies, state organizations and other constituents utilizing federated data management enabled by a common utility layer. This could also encompass data location and workflow orchestration services, as well as enforcement of common rules and processes for data contribution, updates and access. As a result, the paradigm of the NHCD changes from a "single source of truth" to a connected and distributed single source of truth and mitigates the risk of the NHCD becoming just one more federal database.

In addition, technologies such as Blockchain should be considered to provide capabilities for transparency, immutability and traceability for data management. Blockchain is potentially a great enabler of community-based collaboration with a high-level of privacy and security.

Submitting data

Organizations should be permitted to delegate NHCD reporting. Delegation of reporting is permitted in PECOS and by many commercial health plans. However, organizations not only should identify the delegated individual(s) but also work with CMS to verify that the individual(s) are permitted to report on behalf of the organization.

We note that role-based access management (RBAM) is a mechanism for restricting access to systems. Allowing administrators to define permissions for authorized users, many organizations use RBAM to provide varying levels of access based on an individual's role and responsibility. This process can protect sensitive data, while giving the individual the access they need to perform their task. CMS can apply this principle to the NHCD by defining a specific set of permissions that apply to a certain type of NHCD user. Thus, permission would not be granted directly to a user, but rather to a specific role. Users can be added or removed from their NHCD roles according to the requirements.

We also recommend CMS explore leveraging appropriate vendors and clearinghouses to serve as intermediaries for bulk data verification and upload or submission to an NHCD. Many of these entities currently serve this function for providers and health plan clients.

Reviewing and verifying data

We believe one method to resolve duplicate or conflicting information reported from different sources is to have the provider themselves review and correct the information. Another option is to leverage outside data sources to resolve duplicate or conflicting information. We also urge CMS to ensure it establishes one point of contact per organization to minimize the chance of duplicating data entries.

It will be critical to verify provider information such as address and phone number for consumers, providers, and health plans. It will also be important to verify digital addresses such as email addresses and endpoints for providers and health plans. Validation through use of third-party data sources should also be considered. We recommend a three-step validation process. The first step is to verify that the data reported is a valid data set and conforms to the reporting fields (i.e., the address reported by the provider includes zip code). Second, the information should be validated through a primary source. For example, if the provider lists the medical school they attended, that information should be

verified with the medical school itself. Finally, where applicable, verification should involve the appropriate relationship. For example, if the provider reports they have medical privileges at an institution, that institution should verify that relationship.

Technical standards

CMS, especially when the NHCD is launched, should support multiple standards and data reporting formats. Uploads via APIs, online portals, excel files, word files, and faxing options should all be offered to ensure that all reporting entities, regardless of their technical capabilities, can be accommodated. At the same time, the Agency should offer tutorials and technical assistance to those reporting entities that wish to transition from manual to, for example, FHIR-based automated reporting.

Pilot testing

Pilot testing of the various functionalities of the NHCD will be critical to its success. It will be important to have providers, health plans, and others test data submission and data access functions and report back to the CMS to allow for improvements to be made to the NHCD and ensure maximum usability. We also recommend creating an ongoing process to allow users of the NHCD to supply feedback on how to improve functionality.

Accessing the NHCD

To maximize the utility of the NHCD for providers, the information should be accessible directly in the provider's workflow, via their EHR. We anticipate EHR software developers will incorporate supporting API technology into their systems, therefore permitting end users to leverage this technology to access NHCD data.

In addition, an increasing number of patients are accessing information related to the delivery of their health care via apps through their phone or tablets. We urge CMS to meet patients where they are and offer app developers the opportunity to develop solutions that meet the needs of their consumers. We anticipate that apps that leverage NHCD data will be developed to serve specific consumers. For example, an app may be created that lists by geographic region all providers that speak a specific language. This potentially would be a important tool for patients, especially those in underserved and disadvantaged communities.

At the same time, appropriate security protocols must be in place to minimize the potential for unauthorized access and use of NHCD data. We recommend CMS follow industry best practices for securing NHCD as it is reported, maintained or transmitted.

Implementation phases

We believe that CMS should implement a phased approach to the development of the NHCD to build stakeholder trust and adoption. We recommend the following approach:

- **Convene** industry stakeholders, including consumers, providers, health plans, vendors, other appropriate organizations, to discuss needs, requirements, capabilities, timelines, and other issues.

- **Assess** state and local level as well as private sector provider data collection initiatives to determine if opportunities exist to learn from their experiences and

leverage these data sources.

- **Review** existing public and private sector provider information databases to determine if harmonization and/or alignment is appropriate.

- **Develop** an NHCD prototype and solicit feedback from industry stakeholders and data requirements, reporting interface, ease-of-use, and other factors.

- **Pilot** test the NHCD with a wide variety of consumers, provider types, and health plans.

- **Stage** the implementation of the NHCD and continuously incorporate feedback from users.

- **Conduct** outreach throughout this entire development process outreach with each impacted industry sector, including consumers, providers, health plans, vendors and clearinghouses, to answer questions, hear concerns, and build trust in the process and final product.

We also recommend that CMS focus initially on use cases related to provider reporting to those federal health plans and programs under direct CMS regulatory control. As CMS can compel these entities to participate, there would be established an immediate benefit to providers for participating and would build trust and confidence in the process. Additional use cases can be explored once the industry has experience reporting federal plan and program data to the NHCD and utilizing NHCD data.

Finally, we urge the Agency to use human-centered design to optimize the usability of the NHCD. Human-centered design is characterized by six key principles that highlight the importance of centering the end user: (i) Understand end users and stakeholders; (ii) Engage with end users and stakeholders throughout; (iii) Test and revise solutions based on end user and stakeholder feedback; (iv) Iterate; (v) Consider entire experience; (vi) Collaborate across disciplines. CMS should employ these principles as it develops the NHCD. We strongly recommend CMS engage with impacted stakeholders all throughout the NHCD development process to ensure that end-user experience, whether reporting data or accessing data, is streamlined, efficient, and effective.

Conclusion

The issues included in the RFI represent a critical step forward in realizing the vision outlined by policymakers in the bipartisan 21st Century Cures Act of 2016. We encourage you to work with WEDI should additional industry input on regulatory provisions be needed and to identify opportunities to educate impacted entities. As a statutory advisor to the HHS Secretary and a multi-stakeholder organization, WEDI offers a unique structure for cross-industry collaboration.

We appreciate the opportunity to share our perspective regarding the issues included in this RFI. We hope our perspectives and recommendations will serve to assist CMS and ASTP/ONC as it moves forward with important health IT initiatives. Please contact Robert Tennant, WEDI Executive Director, at rtennant@WEDI.org with any questions on these comments and recommendations.

Sincerely,
/s/
Merri-Lee Stine
Chair, WEDI

cc: WEDI Board of Directors