May 28, 2024

The Honorable Micky Tripathi, Ph.D., M.P.P.
National Coordinator
The Office of the National Coordinator for Health Information Technology
Department of Health and Human Services
330 C St SW
Washington, DC 20201

Re: 2024-2030 Federal Health IT Strategic Plan

Dear National Coordinator Tripathi:

WEDI is pleased to submit the following responses to the Office of the National Coordinator for Health Information Technology (ONC) proposed *2024-2030 Federal Health IT Strategic Plan.* This plan seeks to move the health care ecosystem in the direction of interoperability and to meet the vision outlined in the bipartisan 21st Century Cures Act (Cures Act). We commend ONC for recognizing the need to improve interoperability to increase access to health care information and for seeking stakeholder feedback on how this best can be accomplished.

WEDI, formed in 1991, is the leading authority on the use of health IT to improve health care information exchange to enhance the quality of care, improve efficiency, and reduce costs of our nation's health care system. WEDI's membership includes a broad coalition of organizations, including health plans, hospitals, other providers, vendors, government agencies, consumers, not-for-profit organizations, and standards development organizations. WEDI was designated in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) legislation as an advisor to the HHS Secretary.

General Comments

We congratulate ONC on reaching its twenty-year milestone. In two decades of ONC leadership, the march toward deployment of effective health IT and a truly interoperable health care system has made significant strides. With this Strategic Plan, ONC has set a very high bar for both the federal government and the private sector to achieve. We fully support the Administration's broad health IT goals, particularly putting patients at the center of the care delivery process by arming them with the health information they need, when they need it. WEDI also endorses each of the six Federal Health IT

Principles outlined in the Strategic Plan. Ambitious but important, these principles will help to shape health IT and facilitate the advancement of a more efficient and equitable health system.

ONC has set out an extremely aggressive framework and set of goals to achieve over the next six years. With this Strategic Plan, ONC seeks to improve the nation's health care ecosystem and meet the vision outlined in the Cures Act of improving access to, and the quality of, information that patients, providers, health plans and other stakeholders have access to make informed decisions.

While in agreement with this framework and set of goals, we believe the Strategic Plan can be modified to ensure that health care stakeholders gain quicker access to more accurate and pertinent patient information. As well, there must be increased recognition that the sharp rise in inappropriate disclosures of patient information and cyberattacks threatens to weaken our health care system and undermine the public's trust in electronic health data exchange.

Specific Comments

We submit the following comments and recommendations on the Strategic Plan to assist in facilitating the adoption and deployment of equitable, safe, effective, secure, and interoperable health IT.

ONC Strategic Plan Reference
Federal Health IT Principles. Increase health equity across all populations.

WEDI Response
We fully support the federal Health IT principle of increasing health equity across all populations. Our own Health Equity Workgroup provides a forum for the discussion of health equity, social demographics, and social determinants of health (SDOH) with the focus on improving the equity of health care delivery and payment. The Workgroup focuses on business processes and workflows for the capture, exchange, and analysis of health equity, social demographics, and SDOH data and seeks to promote a broader understanding of the impact of SDOH and social demographics on health equity.

As we are all aware, individuals in some racial and ethnic minority groups experience higher rates of poor health and disease for a range of health conditions, including diabetes, hypertension, obesity, asthma, heart disease, cancer, and preterm birth, when compared to their Caucasian counterparts. In addition, the lower an individual's socio-economic position, the higher their risk of poor health. Health inequities are systematic differences in the health status of different population groups. Ensuring equity throughout the health care delivery process should continue to be a priority for the federal government.

ONC Strategic Plan Reference
Improve Health IT Users' Experiences and Outcomes (pg. 2).

WEDI Response
We recommend that ONC include in its priorities the establishment of clinical and administrative data feedback loops. Feedback loops can drive improvement and be another incentive for health IT acquisition and deployment.

To ensure a feedback loop performs optimally within its given workflow, there are certain elements it should include. First the data must be transmitted to the end user in a timely manner. Providers and health plans are required to submit various types of quality and performance data. It is critical that they receive feedback on this submitted data as quickly as possible. This will allow them to take the appropriate action, based on the feedback received. And second, and closely related, the data included in the feedback loop must be appropriate and actionable. Should the feedback received by the provider or health plan not be relevant and useful, the incentive to submit data on the front end will be diminished and reduced attention will be paid to the data included in the feedback response.

ONC Strategic Plan Reference
Federal Health IT Principles. Encourage innovation and competition.

WEDI Response
We appreciate the inclusion of encouraging innovation and competition. These attributes will lead to the development of robust and effective health IT solutions. At the same time, however, we urge ONC to emphasize the agency's oversight and enforcement role. The draft Strategic Plan does not sufficiently underscore the importance of ONC oversight and enforcement to achieve interoperability and deployment of effective health IT. There is concern that some certified health IT products are not able to replicate the ONC certification requirements in the real-world clinical environment. The Strategic Plan should discuss specific processes and actions, including the imposition of significant monetary penalties, that ONC will use as a deterrent to unfair business practices or for any vendor not providing the functionality that the product was certified to support.

ONC Strategic Plan Reference
Federal Health IT Principles. Privacy and Security: Provide tools, guidance, and regulations to build trust and protect individuals' health information from misuse.

Federal Health IT Strategic Plan Framework GOALS AND OBJECTIVES. Goal Four: Connect the Health System with Health Data

WEDI Response
While we are pleased to see that "privacy and security" was included as one of the Federal Health IT Principles, we recommend that ONC consider including this issue as an addition to the four Goals and Objectives outlined in the Strategic Plan (i.e., "Ensure

Privacy and Security of Electronic Health Information"). At a minimum we recommend ONC rename goal number four to be "Securely Connect the Health System with Health Data" to emphasize the importance of security in the Strategic Plan.

Health care organizations today are greater targets for theft than organizations in other sectors for a few important reasons. The personal health and research information facilities hold are high value commodities to cyber criminals, including nation state actors. Decentralized information systems, where a vendor may use the services of one or more subcontractors, provide for a greater number of potential access points for incursion, putting patient care and privacy at risk. Regardless of their size, health care organizations make attractive cyberattack targets. First, they are financially lucrative targets because of the value of protected health information. Since attackers adjust ransom amounts to the perceived ability of the target to pay, attackers often will hold health information systems hostage until they have extracted maximum ransom payments, utilizing sophisticated tactics to transfer breach threats across criminal enterprises.

Many health organizations lack the resources to invest in modern, secure IT systems and harden cybersecurity defenses, often relying on outdated or legacy systems that are vulnerable to exploitation. Health organizations can also lack the capacity to respond to and mitigate cyberthreats, which increases the harm caused by cyberattacks as well as the probability of paying ransoms. With every high-profile attack comes the potential erosion of the patient's trust in the overall health care system. No health care organization is immune to the threat of cyberattack and countering these threats will require a collaborative effort between the private and private sectors.

ONC Strategic Plan Reference

Goal 1, Objective A. The federal government plans to: "Protect the privacy and security of EHI in circumstances beyond those addressed by all applicable federal and local regulations and statutes" so that "Individuals are better informed about how their information will be used in circumstances where Health Insurance Portability and Accountability Act (HIPAA) Rules do not apply (e.g., consumer health applications) and can expect that their health information is safeguarded no matter where and how it is used."

Goal 2, Objective C. The federal government plans to: "Foster a safe and secure health application market" so that "Health care providers and patients benefit from routine use of standardized APIs to appropriately and securely share EHI."

WEDI Response

WEDI fully endorses the use of Application Programming Interface (API) technology to enhance interoperability and give patients access to their health information. However, we continue to be concerned about the security implications associated with the deployment of APIs and we appreciate ONC including this issue in the Strategic Plan. Patients must be the primary authority in designating rights to access, exchange, and use of their data, but other stakeholders have an important role to play as well. ONC

must assist in the design of a process that gives patients the assurance that a third-party application has met a minimum level of security.

We note that some covered entities (CEs), including health plans, physician practices and inpatient facilities, have already built themselves or have contracted with business associates (BA) to develop patient access APIs and apps and are actively promoting their use. Specifically, these apps deployed by CEs 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 and security standards applicable to the large percentage of third-party app developers not associated with CEs and therefore not covered under HIPAA. In addition, there currently is no federally recognized accreditation or certification process for these apps.

A Pew Charitable Trust survey found that nine out of ten Americans are concerned about the privacy of their health data when not protected by HIPAA or other federal regulations.[1] HHS through its recent HIPAA modification proposed rule,[2] appears be seeking a new avenue for requiring CEs to transmit ePHI. HHS, in this proposed rule, requests comments on whether CEs should be required to educate or warn individuals that they are transmitting PHI to an entity that is not covered by the HIPAA privacy and security rules.

Consumers 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. 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 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, with patients relying on HIPAA to ensure that the confidentiality of their information is maintained.

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 Cures Act, 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 BA agreement. The deployment of effective federal policies is critical to assist in facilitating this trust framework.

---

[1] B. Moscovitch, Americans Want Federal Government to Make Sharing Electronic Health Data Easier, The Pew Charitable Trusts (September 16, 2020).

[2] Federal Register Vol. 86, No. 12, Thursday January 21, 2021: Proposed Modifications to the HIPAA Privacy Rule To Support, and Remove Barriers to, Coordinated Care and Individual Engagement.

The Centers for Medicare & Medicaid Services' (CMS) own Blue Button 2.0 program recognizes the importance of third-party apps maintaining strict privacy protocols. For example, the Blue Button 2.0 Production Access Checklist[3] 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 permitted third-party API access to Medicare Fee-For-Service claims data through the API once their solution has been approved for production. This program promoted the industry standard Fast Healthcare Interoperability Resources (FHIR), specifically the Bulk FHIR specification. We note that health IT implementers preparing to onboard the DPC production environment were 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.[4]

ONC and its federal partners must ensure patients are educated on their rights and responsibilities regarding APIs, and to the potential threats to their data. We believe this issue is and will continue to be a critical foundation for health IT in the next six years and we suggest it be more thoroughly addressed in the Strategic Plan. Loss of confidence by patients, care givers, providers, and others in API-facilitated data exchange could impact the deployment and use of health IT.

ONC Strategic Plan Reference
Goal 2 Objective (D): "to "Providers experience reduced regulatory and administrative burden."

WEDI Response
We fully support the decision by ONC to include Goal 2, Objective D "Providers experience reduced regulatory and administrative burden." To highlight this area of health care reform reinforces the importance of decreasing burden and cost in our care

[3] https://bluebutton.cms.gov/checklist/
[4] CMS Data at the Point of Care "Terms of Service"

delivery system. We recommend that this section be modified to include other stakeholders, such as health plans. Decreasing administrative burden for all participants in the system frees up resources that can be better targeted at patient care or lead to decreased costs for patients.

In addition, we urge ONC to, in collaboration with other federal agencies, implement specific policies that will reduce regulatory and administrative burden. ONC and CMS have requested stakeholder input on numerous occasions regarding opportunities to reduce burdens. We appreciate the focus on these issues and recommend ONC, CMS and other federal agencies take tangible steps to move beyond simply outlining the many areas of provider burden and take specific policy actions to alleviate these challenges. As an example, despite being mandated by congress in both HIPAA, enacted in 1996 and the Affordable Care Act of 2010, HHS has not yet issued a final rule implementing a national standard for electronic attachments. Currently, exchanging clinical data in support of transactions such as claims, and prior authorizations is burdensome and costly. This administrative standard is critical if the health care industry is to effectively and efficiently exchange clinical data electronically.

The ONC Strategic Plan focuses very heavily on improving clinical workflows, but less attention is paid to the opportunity to leverage health IT to automate administrative transactions. If properly incentivized and deployed, health IT (including the use of artificial intelligence) can dramatically increase the automation of administrative transactions, including the reporting of quality measures and other data submission requirements. Automating what currently are manual administrative processes increases the health IT return on investment for stakeholders and will help incentivize them to make the necessary resource investments.

ONC Strategic Plan Reference
Goal 2 (D): "to "Providers experience reduced regulatory and administrative burden." The federal government plans to Leverage health IT to standardize data and processes related to electronic prior authorizations to allow for increased automation" so that Health care providers experience reduced administrative burden and improved timeliness of prior authorization decisions."

WEDI Response
While we appreciate ONC including the issue of standardizing data and processes related to electronic prior authorizations, it may not be appropriate to reference this in the future tense ("plans to"). With publication of a final rule[5] on Feb. 8, 2024, CMS has established requirements for impacted stakeholders to adopt three FHIR API standards (Coverage Requirements Discovery, Documentation Templates and Rules, and Prior

[5] Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Advancing Interoperability and Improving Prior Authorization Processes for Medicare Advantage Organizations, Medicaid Managed Care Plans, State Medicaid Agencies, Children's Health Insurance Program (CHIP) Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans on the Federally-Facilitated Exchanges, Merit-Based Incentive Payment System (MIPS) Eligible Clinicians, and Eligible Hospitals and Critical Access Hospitals in the Medicare Promoting Interoperability Program Final Rule, published in the Federal Register on Feb. 8, 2024.

Authorization Support). We recommend the Strategic Plan be modified to reflect that ONC will seek to "support the implementation" of this CMS final rule.

ONC Strategic Plan Reference
Goal 2 Objective C Health care is improved through greater competition and transparency. The federal government plans to "Make care quality and price information available electronically" so that "Individuals can easily access, understand, and use quality and price information to make care planning decisions." The federal government plans to "Educate health care consumers on the availability of quality and price information" so that "Health care consumers can use this information to shop for care based on value."

WEDI Response
Signed into law as part of the Consolidated Appropriations Act of 2021, the No Surprises Act (NSA) removed a significant financial challenge for individuals and increased cost transparency. As we have emphasized in our previous communications to HHS, WEDI strongly supported the overall goals of the No Surprises Act which guarantees individuals are not burdened by unexpected medical bills and ensures that consumers have improved access to health cost information.

Given the current challenges around certified technology adoption for providers and their vendors and the need to address existing burdens associated with its adoption, ONC should engage with the health IT community to review existing ONC Health IT Certification Program criteria that could enable greater adoption across the provider community, including a focus on equity and adoption for providers that may face resource challenges when adopting health IT.

To minimize implementation burden it will be critical to leverage existing or forthcoming standards. Providers and health plans are moving forward with standards-based APIs, but their use is far from ubiquitous. Smaller organizations in particular face challenges implementing new technologies. Any standard adopted for the Advanced Explanation of Benefits and Good Faith Estimation and associated workflows will be new for the industry.

With these factors in mind, we recommend the Strategic Plan reflect that the federal government explore opportunities to meet the goals of the legislation while addressing the expected administrative burden associated with the NSA data exchange requirements. Also, the Strategic Plan should recognize the need to develop an implementation glidepath that best meets the needs of providers, facilities, health plans, and the patients they serve.

Further, health care consumers, particularly those in underserved and marginalized communities, will require education regarding not only the price transparency requirements of the NSA, but more importantly, how to leverage pricing and other information, such as quality data, to better inform their health care decisions. In addition, we recommend the Strategic Plan include a reference to working with public and private

sector stakeholders to develop and disseminate educational materials that can assist these individuals understand their rights and how they can best leverage cost, quality, and other data. Reaching individuals where they are and in their preferred language should be a priority.

ONC Strategic Plan Reference
In Objective B (Individuals and populations experience modern and equitable health care) the federal government plans to "Promote education, outreach, and transparency about the use of artificial intelligence (AI) technologies" so that "Individuals and health care providers are better informed about the use of AI technologies in health care and have transparency into performance, quality, and privacy practices."

Goal 2 Objective D. The federal government plans to: "Promote the safe and responsible use of AI tools" so that "Health care providers and patients experience streamlined, more efficient care delivery supported by Decision Support Interventions (DSI)."

WEDI Response
We appreciate ONC including AI in the Strategic Plan. There is near universal recognition that AI has the potential of transforming the health care landscape. However, we believe the focus of AI for the federal government should go beyond simply promoting education, outreach, transparency, and promoting safe and responsible use of AI.

AI is currently deployed by providers and health plans and the vendors that support them. We anticipate that the increased exchange and use of electronic health data will signal the increased deployment of AI in the sector. Currently, the most common applications of AI in health care include diagnosis and treatment recommendations, patient communication, engagement and adherence, and administrative activities. Although there are some examples where AI may perform health care tasks as well or better than humans, there remain critical implementation issues that need to be addressed prior to wide-scale deployment of this technology.

From the patient's perspective, the goals of using AI in the delivery of health care services are to improve outcomes and reduce overall cost in the health care system and direct costs to the consumer. Health care is already expensive on a macro level as well as an individual one for many consumers and many fear that new AI-based technologies will drive up costs. At the same time, AI systems can be used to inform the patient regarding the availability of providers and the expected cost related to medical services.

AI also has the potential of improving provider directories and accurately signal if a provider is accepting new patients. With cost transparency being an important issue, AI can be leveraged by patients to give them an accurate estimate of the costs of a medical service, treatment, medication, or device. Among many potential uses of AI,

health plans may wish to leverage AI in their cost calculators by using historical claims data of what services cost.

Further, AI has the potential of assisting clinicians and improving patient care. The dominant applications of Natural language Processing (NLP) involve the creation, understanding and classification of clinical documentation and published research. NLP systems can, for example, analyze unstructured clinical notes on patients, prepare reports (e.g., on radiology examinations), transcribe patient interactions and conduct conversational AI.[6]

We urge ONC to consider including in the Strategic Plan a reference to appropriate "deployment of AI" to improve data collection and use. We also recommend ONC include "AI research" in its final Strategic Plan. Government research into AI and health care should be accelerated and could include: (i) Whether AI in health care creates or reduces costs for patients and other stakeholders; (ii) If and how new scientific and clinical findings should be shared through open-source methods; (iii) The ability for AI to improve administrative and clinical performance; and (iv) The need for continuous training by data from clinical studies and other research sources.

ONC Strategic Plan Reference
Goal 2 Objective A. The federal government plans to: "Use health IT to support payment for high-quality, value-based care" so that "Health care providers deliver high-quality care in a transparent, modern, and competitive market."

WEDI Response
We commend ONC for recognizing the role health IT can play in supporting value-based care. To effectively coordinate care and achieve the goals of value-based care, providers must leverage health IT to exchange patient information between other providers, other care settings, health plans, and patients themselves. Getting high quality, actionable data into the hands of those that need it, when they need it, should be a priority for ONC as it develops, for example, future versions of its health IT certification programs.

ONC Strategic Plan Reference
Goal 2 Objective A. The federal government plans to: "Support efforts to address patient identity and record linking solutions so that "Potential medical errors are avoided, and burden related to manual data matching is reduced."

WEDI Response
Accurate patient record matching is a critical component of health IT and interoperability. At a minimum, if records are not matched accurately there is administrative waste and needless cost. More importantly, mismatched records can

[6] For additional opportunities to leverage AI for patient, providers, ana health plans, access WEDI's response to the U.S. Senate Health, Education, Labor and Pensions Committee draft white paper entitled "Exploring Congress' Framework for the Future of AI: The Oversight and Legislative Role of Congress Over the Integration of Artificial Intelligence in Health, Education, and Labor."

lead to medical errors and harm to the patient. Although mandated in HIPAA, the creation of a national patient identifier has been put on hold and congress continues to prohibit the federal government from working on this issue.

Those opposed to national strategy on patient identification cite privacy concerns as one of the main arguments against lifting the ban. However, we are concerned that patient privacy may be impacted because there is no national strategy. Currently, patients are required to disclose a significant amount of individually identifiable information to each health care provider they encounter to ensure an accurate match of the patient to their medical record occurs. Unauthorized disclosures also can occur as a record from one patient is inadvertently merged with the record of another patient with, for example, the same name and or same birth date. The medical consequences of such an occurrence could be catastrophic for the patient.

We are hopeful that the removal of Section 510 from the Labor-HHS appropriations bill will provide HHS (through ONC) with the ability to evaluate a range of patient identification solutions and enable it to work with the private sector to explore potential challenges and identify a national strategy around patient identification and record matching that protects patient privacy and is cost-effective, scalable, and secure.

ONC Strategic Plan Reference
Goal 2 Objective E. The federal government plans to: "Study and seek to optimize the use of health IT in supporting health care, public health, and human service provider workflows" so that "Health care, public health, and human service providers experience better efficiency, convenience, and outcomes in workflows supported by health IT."

WEDI Response
We believe there is an opportunity to augment Objective E by including a discussion of a health IT return on investment (ROI). For stakeholders to prioritize the transition to health IT, they need to know that there will be value to their organization, their members, their customers, and/or their patients. Thus, accurately measuring the clinical value and financial ROI of Health IT should be a priority for ONC and included in its Strategic Plan.

Similarly, we suggest the Strategic Plan include a focus on prohibiting unfair vendor business practices. Interoperability will stall and provider support will be reduced should health care organizations be the target of unfair vendor business practices. ONC should include in the final Strategic Plan an objective focused on prohibiting vendors from imposing unreasonable fees or requirements.

ONC Strategic Plan Reference
Goal 2 Objective E. The federal government plans to: "Support expanded use of secure telehealth, including audio-only telehealth" so that "Health care providers and patients can easily access and use telehealth, when appropriate, to reduce disparities in health care access and health outcomes."

WEDI Response
We fully support the inclusion of telehealth in the Strategic Plan. Under the constraints of social distancing, closings, and further efforts to prevent the spread of COVID-19, Telehealth rapidly became more mainstream and will likely impact the way in which many providers practice medicine going forward. ONC should investigate the value of telehealth for various populations, the constant evolution of telehealth initiatives, and what does the future holds as it relates to telehealth reimbursement and policy now that the public health emergency has ended.

The WEDI Telehealth Workgroup identified another issue that ONC should explore. The increased utilization of telehealth services, driven by the pandemic and public health emergency response, exposed the need for integration of telehealth patient records into the providers electronic health record (EHR). The Workgroup identified the following benefits to improved telehealth integration into the EHR: (i) Having a complete medical record in one system; (ii) Documenting all patient services in one location; (iii) Gathering data in one location for quality, public health and other tracking purposes; and (iv) Having a patient's complete record in one system for administrative needs.

Integration is complicated when a provider's telehealth system and EHR are not integrated or when patients use standalone telehealth applications.
The lack of integration can increase provider workload, impact quality and patient safety, result in unstructured data being included in the EHR, and impede coordination of care. Those in rural areas are more likely to struggle because of challenges in achieving patient engagement, shortcomings in technology and the cost of achieving integration.

Conclusion

In conclusion, WEDI strongly supports the objective of deploying health IT to improve the sharing of clinical and administrative data to decrease administrative burden and improve the care delivery process. There is work to be done to overcome technical, legal, and logistical barriers to the widespread and effective use of health IT. Through implementation of appropriate policies, processes, and incentives, as well as outreach and education to patients, providers, health plans and other key stakeholders, we believe that the nation's health IT infrastructure can achieve the goals and vision laid out in the Cures Act.

With the publication of this *2024-2030 Federal Health IT Strategic Plan*, ONC has taken on the formidable task of reshaping public policy to create a health care environment that leads to improved patient care and more efficient delivery of that care. We look forward to continuing to work with ONC and other federal agencies to facilitate the continued transition to effective health IT and ensure that the promise of improving the nation's health care system through technology becomes a reality.

As the collective voice of the health care industry on health IT issues, we are pleased to continue our important partnership with ONC and assist in the development and

implementation of a national health IT policy. Please contact Charles Stellar, WEDI President and CEO, at 202.329.9700 or cstellar@wedi.org with any questions you may have regarding the comments and recommendations we have offered in this letter.

Sincerely,
/s/
Ed Hafner
Chair, Board of Directors

cc: WEDI Board of Directors