601 Pennsylvania Avenue, NW   T 202.778.3200
South Building, Suite 500   F 202.331.7487
Washington, D.C. 20004   ahip.org

May 28, 2024

Micky Tripathi, Ph.D.
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 Dr. Tripathi:

AHIP[1] appreciates the Office of the National Coordinator for Health Information Technology's (ONC) ongoing work to advance the use of technology to improve health and health care. We congratulate you on ONC's 20th anniversary and the strides the agency has made towards creating a truly interoperable health care system. Patients deserve high-quality, equitable, and affordable care delivered by health care providers and health plans working together with patients so that they make informed health and healthcare decisions. With this goal in mind, we are pleased to offer the following comments on the proposed *2024-2030 Federal Health IT Strategic Plan.*

First, we applaud the Strategic Plan's focus on protecting patient privacy and enhancing cyber security of patients' data including electronic health information (EHI) shared with entities not covered by the Health Insurance Portability and Accountability Act (HIPAA). While we strongly support an individual's right to manage their health information, **we cannot offer the false choice of data sharing or robust protections. We must ensure that a person's data is kept private and secure regardless of who holds it and whether it is covered by HIPAA.**

Second, we support the Strategic Plan's emphasis on using technology to reduce administrative burden. AHIP agrees with the vision laid out in ONC's and the Center for Medicare & Medicaid Service's Interoperability rules. Improved interoperability can reduce the effort of valuable but burdensome activities such as prior authorization and quality measurement. **Technology allows us to reduce the time providers spend on these activities while protecting their essential role in promoting safe, effective, and evidence-based care.**

However, how these policies are implemented will be key to their success. Technologies such as the Prior Authorization Application Programming Interface (API) will only successfully reduce burden if all parties involved use them. **Electronic health record vendors should be required**

---

[1] AHIP is the national association whose members provide health care coverage, services, and solutions to hundreds of millions of Americans every day. We are committed to market-based solutions and public-private partnerships that make health care better and coverage more affordable and accessible for everyone.

to build and health care providers must use the electronic prior authorization APIs offered by health plans.

We also need the infrastructure to support these policies. **For example, we need a National Healthcare Directory that includes digital endpoints so health plans and providers can connect to exchange data.** We also encourage ONC to explore ways to utilize the Trusted Exchange Framework and Common Agreement (TEFCA) to facilitate processes such as quality measurement. A use case that allows plans to use TEFCA to support measurement could reduce burden on all stakeholders.

We also appreciate the Strategic Plan's vision to leverage HIT to promote health equity. Increasing the availability and interoperability of data on social determinants of health (SDOH) and better connecting community-based organizations (CBOs) will help all stakeholders address patients' social needs. AHIP has been working with members and other health care stakeholders to modernize and enhance demographic data standards so they are culturally sensitive, sufficiently granular, and aligned across stakeholders. Our goal is to facilitate the collection of actionable, accurate, interoperable to promote health equity. **We look forward to working with ONC and other agencies to adopt and implement these revised standards in the United States Core Data for Interoperability (USCDI) and other federal data standards.**

Finally, we appreciate that the Strategic Plan acknowledges the opportunity and risks that Artificial Intelligence (AI) provides. We agree that transparency will be essential to minimize the potential harms from AI, including from algorithmic bias. Successful use of AI to enhance high-quality, equitable, and affordable care will depend on responsible approaches to both AI development and AI deployment. **The federal government should take a risk-based approach to regulating AI enhances transparency while allowing innovation and protecting intellectual property.**

We appreciate the opportunity to provide feedback on the proposed Strategic Plan. We support the vision ONC has laid out and offer our detailed comments below to facilitate successful implementation. AHIP and our members look forward to working with ONC to operationalize the Strategic Plan to advance health and health care and meets the needs of all stakeholders. If you have any questions, please contact me at (202) 778-3246 or at dlloyd@ahip.org.

Sincerely,

Danielle A. Lloyd

Danielle A. Lloyd
Senior Vice President, Private Market Innovations & Quality Initiatives

Goal 1: Promote Health and Wellness

<u>Objective A: Individuals are Empowered to Manage their Health.</u>

Protect the Privacy and Security of EHI

AHIP and its members wholeheartedly support the underlying goal of moving toward a health care system in which data flow seamlessly among trusted parties to the benefit of patients. We also recognize the potential and support the goal of leveraging application programming interfaces (APIs) to help individuals access their data and take control of their health and health care.

However, with these new opportunities come new threats to patient privacy. New entity types, such as application (app) developers, that are now common in the marketplace were not contemplated, let alone included, as covered entities within the Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health (HITECH), or 42 CFR Part 2 rules. AHIP fully supports efforts to improve individuals' access to their protected health information (PHI). However, to effectively safeguard that information in an app environment, we believe Congress should pass a national consumer privacy framework that fully preempts the patchwork and proliferation of conflicting state privacy laws and provides for a clear and complete carveout of HIPAA covered entities. This is critical to ensuring health care data obtained by non-HIPAA regulated third-party apps and services through these APIs continue to be held to high privacy and security standards. **We support the Strategic Plan highlighting a strategy to "Protect the privacy and security of EHI in circumstances beyond those addressed by all applicable federal and local regulations and statutes."**

As personal health information becomes more freely available, privacy and security are essential. To operationalize this commitment, AHIP's Board of Directors and its Chief Medical Officers leadership team released core guiding priorities and a detailed roadmap to further protect the privacy, confidentiality, and cybersecurity of consumer health information.[1]

One growing threat to patient privacy is the ability to re-identify data that has previously been de-identified. As more personally identifiable information is available, it is increasingly possible to link data sets to identify an individual's data. One strategy to prevent de-identified data from being re-identified is to share the minimum necessary personally identifiable information. The information included in the USCDI must be shared by providers and most payers, at a patient's request, with third-party applications (apps) that are generally not governed by the Health Insurance Portability and Accountability Act (HIPAA) and are permitted by patients to use data for secondary purposes. This exchange, given present technological constraints, is all-or-nothing. Thus, extreme caution should be exercised and the notion of minimum necessary applied to the inclusion of data elements. AHIP has noted in our previous public comments our concerns about the inclusion of personally identifiable information such as Member Identifier, Subscriber Identifier, Relationship to Subscriber, and Group Number as elements in the USCDI. Such

---

[1] https://www.ahip.org/news/press-releases/ahip-outlines-priorities-and-roadmap-for-protecting-privacy-and-security-of-consumer-health-information

information, when combined with current USCDI version 1 data elements, such as First Name, Last Name, Date of Birth, and Current Address, could risk a person's privacy and even safety.

AHIP supports expanding legal requirements to entities that collect, use, disclose, or store individuals' health and health-related information (including social needs). To complement transparency and interoperability efforts, privacy requirements should be designed and applied across all entities that have access to health information so that existing privacy protections are not weakened. While the robust and tailored HIPAA and HITECH laws should remain the applicable governing law for covered entities, we recommend that Federal Trade Commission (FTC's) authority and scope of oversight be expanded to cover all entities outside of HIPAA with comparable robust protections.

Develop Educational Resources

We also appreciate the Strategic Plan including a strategy to "Develop educational resources for choosing and using secure technologies that incorporate privacy protections." CMS and OCR should develop materials for consumers to provide information about their rights under HIPAA and the interaction with these innovative technologies and modern processes. HHS, collaborating with the FTC, should take the lead in making consumers aware of the risks and implications of granting data sharing access to third-party apps not regulated by HIPAA and how to lodge complaints specific to those apps. Given CMS' experience implementing the Medicare Blue Button 2.0 initiative as well as the associated consumer education campaign, it is well-situated to leverage lessons learned and apply them to this broader effort including consumer education. This will also provide consumers with a streamlined government resource they can reference throughout their healthcare journeys. CMS could also use its authority to share the information it obtains from its vetting process for Medicare data to establish ratings of third-party apps on its website.

Objective B: Individuals and populations experience modern and equitable health care

Improve Demographic Data Availability

Better data will be foundational to understanding how to improve care and ensuring no one is left behind as we strive to advance health equity. **We support the Strategic Plan's vision that "Data classes and data elements that improve clinical and social determinants are standardized and included in health and human services systems."** Collecting demographic data that better aligns with how people identify and can be exchanged in an interoperable way will allow stakeholders to better detect health and health care disparities and understand how best to care for members of specific populations. To advance health equity, AHIP has been working with members and other health care stakeholders to modernize and enhance demographic data standards so that they are culturally sensitive, sufficiently granular, and aligned across stakeholders. Our goal is to facilitate the collection of accurate, complete, comparable, actionable, and interoperable data that supports better outcomes, fewer disparities, improved patient trust, and enhanced operational efficiency. We look forward to working with ONC and other agencies to adopt and implement these revised standards in the United States Core Data for Interoperability (USCDI) and other federal data standards.

Promote Evidence-Based Digital Therapies

The Strategic Plan aims to "advance the use of validated, evidence-based digital therapeutics and diagnostics." Health plans support the use of evidence-based digital tools with sufficient data on real-world applications to improve patient care and access and to promote the use of innovative treatments. However, we note that several challenges exist to ensuring digital therapeutics are effective and supported by evidence. There has been a rapid proliferation of digital therapies, and the Food and Drug Administration (FDA) regulates only a small subset. Thus, there is little information for health plans, patients, and providers to understand which therapies are safe and effective and how these tools can help with individual treatment plans or needs.

For digital therapies that are reviewed by the FDA, we encourage the agency to leverage the post-market surveillance process to understand the safety, efficacy, and use of digital therapeutics that have been FDA approved. **The FDA should work with technology companies, health care providers, and health plans to determine strategies to monitor treatment failures and potential patient harm.** We also encourage the Department of Health and Human Services (HHS) to identify best practices for clinical use from this data to enable and encourage successful use of digital therapeutics.

While treatments that are not approved by the FDA can be an important part of health care delivery, they must be held to a standard that ensures that a patient gets high-quality, high-value care from their use; digital therapeutics must produce measurable benefits for a patient, as more traditional care would be expected to achieve. For payers to provide coverage of these technologies and providers to use them, we need independent, credible organizations to assist with evaluations of these various technologies. **Thus, we urge HHS to work with the private sector to identify ways in which digital therapies not subject to FDA review can be evaluated broadly and the results shared to facilitate adoption.**

HHS should also consider developing educational resources for health care providers. Such guidance could raise awareness of the potential risks and benefits of digital therapeutics. It could also assist providers in selecting apps they may wish to recommend to consumers as well as help them determine if data brought to them by consumers gathered from apps should be integrated into care decisions.

For all digital therapeutics, threats to privacy are another potential source of patient harm that could arise from digital therapeutics. **Digital tools should be covered by HIPAA or HIPAA-like policies and any data collected from the use of the tool should be stored and transmitted in a protected way.** Data breaches and the exposure of personal health information are risks, and digital therapeutics should uphold the highest levels of cybersecurity and patient protection.

In addition, to foster the development of technologies they must have a clear line of site to not only coverage, but also payment. Without comprehensive coding and billing standards it will be more difficult for technologies to get paid, dampening innovations. In addition, further thought needs to be given to best practices for the architecture of payments using these codes to both

encourage access for beneficiaries and drive efficiency. Finally, education around changes in standards will need to be widespread to ensure there are not inequities in adoption. **CMS should work with stakeholders to develop a cohesive strategy for evolving coding, billing and financing models to meet the needs of new digital technologies and appropriately support their implementation.**

Prioritize Risk-Based Approaches to Responsible AI

The Strategic Plan notes a need to "promote education, outreach, and transparency about the use of artificial intelligence (AI) technologies." As Americans increasingly interact with AI in many facets of life, including across the health system, it is important to create balanced policies that help realize the potential of AI and build trust among patients and stakeholders. We agree that used responsibly, AI has the potential to improve health outcomes, increase access, and achieve meaningful operational efficiencies to lower costs.

As the federal government considers these goals and additional ways to support ongoing innovation while protecting consumers, we recommend prioritizing risk-based approaches built on national, industry-utilized standards. Federal agencies, including the National Institute of Standards and Technology (NIST) and others can help inform new regulatory proposals, including the work of the Office of Science and Technology Policy (OSTP). To date, NIST has been a federal leader in this area and should serve as a resource for individuals and entities as substantive and technical policies are developed and adopted. The private sector has also started to create governance, ethical, and practice standards for organizations developing and deploying AI. For example, AHIP worked with the Consumer Technology Association (CTA) and the American National Standards Institute (ANSI), on the recent development of the consensus-driven standard, ANSI/CTA-2090, The Use of Artificial Intelligence in Health Care: Trustworthiness.[2]

The federal government should also consider ways to leverage existing laws and regulations. There may be situations where existing frameworks may need to be supplemented to account for AI, but there are robust regulatory frameworks towards addressing discrimination in the US today and regulators have already expressed their intent to leverage them when regulating AI applications. Rather than develop numerous, conflicting laws and regulations, the federal government and the states should work together to leverage existing policies to foster transparency while mitigating potential harm from AI.

Additionally, the government should also consider the critical role of public-private partnerships in educating consumers and building public trust in emerging technologies. AI will affect every industry and facet of life. Robust coordination and cooperation between the public and private sectors will allow us to balance responsible AI use with robust consumer protections.

Finally, we support an approach to AI regulation that promotes transparency and trust. Trust is the foundation of AHIP members' engagement with patients and consumers. Health plans build and maintain this trust today in numerous ways, including by protecting the privacy

---

[2] https://shop.cta.tech/products/the-use-of-artificial-intelligence-in-healthcare-trustworthiness-cta-2090

of patient information and promoting tools and resources to support patients' active engagement in their health and well-being. Transparency is a key enabler of trust and is a critical component of successful deployment and use of AI. Patient, consumer, and caregiver education is critical to helping individuals better understand what AI is and how it might be used. For example, ONC and CMS should consider developing resources to explain the new information on decision-support interventions to health care providers.

The core principles of AI transparency and explainability go hand-in-hand and will provide consumers and other end-users with useful, actionable information. For example, developers of high-risk AI tools can utilize plain language examples of how the AI tool was designed and how it forms the basis of its decisions. As appropriate, AI developers and deployers can also provide information on the data used to train the AI tool to contribute to transparency efforts.

However, it is critical to balance the goal of fostering explainability with the need to protect certain types of information. In considering approaches to appropriate AI transparency, it is essential to protect proprietary information, such as intellectual property and trade secrets, as well as confidential information.

Objective C: Communities are Healthier and Safer

Facilitate Data Sharing Between Plans and Providers

We agree with the vision of expanding the flow of health care data to improve population health and address public health challenges. In particular, we support the strategy to "Support EHI sharing between health care providers and organizations serving communities." As a way to facilitate this data flow, we recommend ONC and CMS expand the recently finalized Provider Access API to support a bidirectional exchange of information between providers and payers.

We see three major use cases to this exchange: 1) facilitate the access and sharing of retrospective claims data from payers to providers to support population health and quality measurement; 2) support access and exchange of retrospective clinical information from providers to payers for quality measurement, utilization review, risk adjustment, and fraud detection; 3) enable access and exchange of dynamic data to support patient care, such as identified care gaps to providers and admit/discharge/transfer (ADT) alerts to payers.

These use cases should also be supported by the Trusted Exchanged Framework and Common Agreement (TEFCA). We note that the prior interoperability regulations did create a bi-directional exchange between health plans and providers that could enable plans to proactively support a member's care. For example, while information on ADTs is readily available to providers, it is not available to plans as part of operations. However, plans have seen great value in access to this data to enable alerts to providers and reduce unnecessary readmissions. CMS should set the stage for this aspirational vision in the final rule, but also recognize that sharing of real-time data to support patient care is not yet operationally feasible. The patient care use case would require up-to-date data that can be easily parsed on both the payer and provider sides to support clinician decision-making at the point of care.

Goal 2: Enhance the Delivery and Experience of Care

Objective A: Providers deliver safe, equitable, high-quality, and improved care.

Build the Infrastructure Needed to Support Interoperability

Improving healthcare quality is of the utmost importance to health plans. AHIP believes all Americans deserve high-quality, affordable healthcare and that value-based care (VBC) and alternative payment models (APM) hold promise to achieve better outcomes at lower costs. Health Information Technology (HIT) can ensure clinicians have the information they need to support their decision-making, facilitate quality measurement, and advance the adoption of VBC and APMs.

We support the strategy to "promote interoperable and secure health information sharing through nationally adopted standards." However, to share information in this way, organizations will need to be able to find each and identify the appropriate digital endpoints. We are encouraged by CMS's recent request for information on the creation of a National Directory of Healthcare Providers and Services (NDH). **The NDH will be essential to the success of CMS's and ONC's recent policies to promote information sharing through APIs as information on provider's digital endpoints remains limited.** As noted in CMS's Request for Information many providers still fail to share data on their digital endpoints through the National Plan and Provider Enumeration System (NPPES), despite CMS's efforts to add these fields to the database and require their completion.[3] Without a comprehensive national healthcare directory and requirements for providers to complete the necessary information, implementing the Provider Access API will be challenging.

We also appreciate the federal government's plan to "support efforts to address patient identity and record linking solutions." **CMS and ONC should advance the HL7® FHIR at Scale Taskforce (FAST) initiatives to address the ongoing challenges of patient matching and identity management, digital identity, security and authentication, and access to the necessary digital endpoints.** The ONC Interoperability, Information Blocking, and the ONC Health IT Certification Program Final Rule (Information Blocking Rule)[4], as well as the Interoperability and Patient Access Final Rule and this proposed rule, all establish policies focusing on the connection between each payer, each member/patient, and each individual app developer and/or each individual provider. The FAST initiative, which includes many AHIP members, is actively working to identify common scalability approaches to speed adoption and avoid each stakeholder reinventing the wheel.

Support Value-Based Care

We also support the plan to "use health IT to support payment for high-quality, value-based care." VBC has the potential to both lower costs and improve quality. However, adoption of VBC can lead to a proliferation of quality measures. HIT has the potential to streamline reporting

---

[3] https://www.federalregister.gov/documents/2022/10/07/2022-21904/request-for-information-national-directory-of-healthcare-providers-and-services

[4] RIN 0955-AA01, 84 Fed. Reg. 7424 [March 4, 2019]

and reduce the burden of measurement by facilitating data extraction and submission and promoting multi-payer measure alignment.

To foster alignment across public and private sector payers, AHIP has partnered with CMS to convene to Core Quality Measures Collaborative (CQMC). The CQMC has developed 10 sets of measures that should be prioritized for adoption. Part of the CQMC's work has focused on leveraging digital quality measures (dQMs) to advance the field of measurement while reducing burden and enabling performance assessment in new ways. To facilitate the transition, we recommend CMS and ONC develop a long-term plan on digital measurement with multistakeholder input that outlines the inputs, steps and milestones necessary to protect patient privacy, build the required infrastructure (e.g. the necessary technical standards for both content and exchange, including a potential use case under TEFCA, develop the necessary measures, ensure widespread stakeholder engagement, and mitigate disparities. **CMS and ONC should look to the work of the CQMC to advance digital measurement and to prioritize the development and incremental adoption of dQMs.**

Balance Innovation with Patient Protections and Transparency

We agree that as the use of advanced analytics, machine learning (ML), and AI grows, there is a need to address potential risks while working to optimize the use of these technologies. As the government aims to "Increase transparency and understanding of health data that goes into algorithm-based decision support tools," we recommend an approach that balances the risks and potential of these technologies.

AI and ML have great potential to improve health care. As examples, AI has proven effective at detecting lung cancer and has been used in breast cancer screening methods.[5] It has also been used in developing medicines, particularly for rare diseases and personalized treatments.[6] However, as detailed above, we must balance innovation with patient protections and transparency.

We note that ONC recently finalized a criterion for decision-support interventions (DSIs) for the Health Information Technology Certification Program (Certification Program). This work by ONC represents an initial effort by the federal government into overseeing AI. We support ONC's approach of requiring transparency rather than external review of clinical decision support technologies that engage or interact with certified health IT, such as electronic health records. ONC has focused on providing information on the populations used to train an algorithm to support consumer and provider decision-making. However, this was created for the specific use case of provider use within an electronic health record. To the extent that this framework is carried forward to additional use cases, a risk-based approach should be considered, and relevant stakeholders should be consulted to determine if some customization is

---

[5] A. Brooks, "The Benefits of AI: 6 Societal Advantages of Automation" Rasumessen University (Nov. 4, 2019) available at: https://www.rasmussen.edu/degrees/technology/blog/benefits-of-ai/. See also, S. Bansal, "10 Advantages and Disadvantages of Artificial Intelligence" available at: https://www.analytixlabs.co.in/blog/advantages-disadvantages-of-artificial-intelligence/.
[6] S. Daley, 32 Examples Of Ai In Healthcare That Will Make You Feel Better About The Future (updated July 29, 2020) available at: https://builtin.com/artificial-intelligence/artificial-intelligence-healthcare.

needed given a different context. Furthermore, we encourage ONC to continue working with other agencies and standard development entities to encourage alignment of AI best practices across health care tools.

Support Interoperability of SDOH Data

The strategic plan also notes the federal government plans to "advance standardization and interoperability of social determinants of health data." To truly address social needs and reduce health care disparities, we need national data and exchange standards that permit stakeholders from across the health care industry to report and exchange information. Moreover, such information should ideally be available in real-time and at the point of care, not only when a claim is submitted.

CMS and ONC should explore how to leverage the USCDI and TEFCA to facilitate the exchange of data on social needs in a way person-centered way that protects patient privacy and security and is done with a person's consent. ONC has continued to build on the USCDI and has added several new data classes and data elements related to social determinants of health (SDOH) in the soon to be required USCDI v3, the finalized USCDI v4 and the proposed USCDI v5. These additional data elements could be useful in understanding a member's social risks and needs. However, before these elements are implemented, more work needs to be done to standardize SDOH related data. AHIP and its member plans are actively working with HL7's Gravity Project to move toward standardized data collection and exchange as quickly as possible. We believe such information is pivotal to identifying health disparities and ensuring care is delivered in a more equitable manner. ONC and CMS could also explore ways to use USCDI+ to facilitate the collection and exchange of sociodemographic data. ONC and CMS should also explore ways to encourage a broad range of organizations to participate in TEFCA and exchange necessary information on a patient's social needs and risk. TEFCA could facilitate a flow of information to all parties with a role in supporting a patient. For example, data on social risk could be available to a health care provider planning a care transition for a patient, to a case manager at a health plan outlining what supports a member may need, or to a community-based organization receiving referrals for social supports.

Finally, CMS and ONC have not placed similar requirements for health care providers to share USCDI with health plans. By developing parallel requirements for providers to share data with payers and payers to share data with providers, CMS could ensure that data flows across the system to support patient care. By incorporating payers in data sharing efforts, health plans could help to manage a person's social needs and facilitate interventions to address them. A person's demographic and social needs data could help health plans take a more active role in addressing their members' needs. CMS and ONC should also require providers to share such data with payers to allow payers to take a more active role in assisting with social needs.

Objective B: Patients experience expanded access to quality care and reduced or eliminated
health disparities.

Support Access to Telehealth

AHIP agrees that health disparities must be identified and addressed, and that HIT could play an
important role in expanding access to quality care for all patients. We appreciate the Strategic
Plan including the government's plan to "support expanded use of secure telehealth, including
audio-only telehealth."

Our collective experience has demonstrated that telemedicine is an important health care
innovation. Telemedicine's value as a modality is supported by recent data —it is a cost
effective, convenient means of delivering high quality care, particularly to traditionally
underserved areas,[7] and can expand access to care and reduce disparities, especially for rural
populations where there is limited access to in-person care, including specialty care.
Telemedicine can help eliminate barriers for patients such as transportation, childcare needs, time
needed off work, and other challenges.[8] AHIP strongly supports the use of telemedicine and our
members are committed to expanding access to virtual care.

AHIP strongly supports the use of telemedicine and our members are committed to expanding
access to virtual care. The SDOH that impact many people are why telemedicine provides a
lifeline. Transportation, childcare, work schedules, and other challenges, including concerns
about stigma, may prevent people in certain communities from accessing in-person care. The
convenience of telemedicine is often cited as the reason people in underserved communities
choose virtual care.[9]

As the federal government considers way to advance the use of telehealth, we strongly support
policies that enable continued innovation in telehealth by ensuring health plans and other
stakeholders have flexibility to introduce new products and services that can benefit patients,
while working to protect patient privacy and data security and combating fraud, waste, and
abuse. Telehealth can be an important tool to improve care delivery, and the technology should
be leveraged to coordinate patient care across different providers, settings, and types of
interaction, including audio-only services. Health plans are encouraged by the expansion and
opportunities enabled by the growth in telehealth and are working to further support its clinically
appropriate use for their members.

It is important that the continued proliferation of tools such as telehealth occur in an equitable
manner, rather than continuing to exploit the "digital divide." There are gaps in access and
awareness of digital tools, which are especially relevant across different geographies, race and

---

[7] Butzner M, Cuffee Y. Telehealth Interventions and Outcomes Across Rural Communities in the United States:
Narrative Review. J Med Internet Res. 2021 Aug 26;23(8):e29575. doi: 10.2196/29575. PMID: 34435965; PMCID:
PMC8430850.

[8] Oluyede L, Cochran AL, Wolfe M, Prunkl L, McDonald N. Addressing transportation barriers to health care
during the COVID-19 pandemic: Perspectives of care coordinators. Transp Res Part A Policy Pract. 2022
May;159:157-168. doi: 10.1016/j.tra.2022.03.010. Epub 2022 Mar 7. PMID: 35283561; PMCID: PMC8898700.

[9] https://www.ahip.org/news/press-releases/new-survey-americans-value-the-convenience-and-simplicity-of-
telehealth-for-their-care

ethnicity, and ages. Ensuring appropriate distribution, access, and training on these tools is paramount to advancing health care. We support efforts to enhance digital health literacy; low digital health literacy is a significant obstacle in achieving equity, and many older adults and individuals with low digital health literacy experience gaps in access to the health care they need. **We encourage CMS to create similar digital health screening and education programs for Medicare FFS beneficiaries as proposed under Medicare Advantage.**

There is also a need to improve the documentation and coding of digital literacy. AHIP supports the addition of ICD-10 codes related to digital literacy under Z55 (Problems related to education and literacy) as digital literacy can play a significant role in empowering patients to be active participants in their health, promoting accessible care, and ultimately improving health outcomes. Digital illiteracy can also be a key driver in perpetuating health inequities as it keeps individuals (often from vulnerable and marginalized communities, such as individuals with low-incomes, seniors, rural residents, individuals with limited English proficiency, people with disabilities, among others) from being able to find and access information that could impact their health.[10] Adding a way to capture this information through ICD-10 codes would allow care team members to have the information they need to better address patient's needs.

Promote health IT that supports greater integration of health care and human services

We also support the vision to integrate health care and human services technologically. Reducing health disparities and promoting health equity will require addressing health-related social needs and better integration could facilitate referrals from health care providers to community-based services.

As noted above, we support efforts to "advance the collection and use of standardized SDOH data (including preferred languages) to reduce health and health care inequities and disparities." A better understanding of the challenges patients experience will help their care teams address their needs and help them achieve optimal health outcomes. We agree that standardized, interoperable SDOH data will be key to advancing health equity. We also appreciate the vision to improve data collection and recommend the government consider ways to leverage interoperability to allow patients to report data once and share it among their health care teams, including their health plans. This will reduce the burden on all stakeholders, but most importantly for patients who may be understandably hesitant to continually discuss sensitive information. **We also strongly recommend the government work with stakeholders to promote person-centered, culturally sensitive data collection efforts.**

Objective C: Health care is improved through greater competition and transparency.

Adopt Cost Sharing Policies that Promote Competition

As part of goal 2, objective C, the strategic plan states the federal government will make care quality and price information available electronically. Consumers and patients deserve easy access to the actionable information they need to make informed decisions about their health and health care for themselves and their families, including where to seek high-value care.

---

[10] https://academic.oup.com/jamia/article/11/6/448/696858

HIT could help ensure all stakeholders, especially patients, have the data they need to make informed decisions about cost and affordability. However, requiring public disclosure of pricing data could have potential negative competitive effects that could hinder fair negotiations and drive-up prices. According to the Federal Trade Commission (FTC), "…transparency is not universally good. When it goes too far, it can actually harm competition and consumers. Some types of information are not particularly useful to consumers, but are of great interest to competitors."[11] Negotiated payment rates, including those delineated by billing codes for individual providers and plans, would unbalance leverage during negotiations, hinder market competition, increase prices and is inconsistent with existing Medicare Advantage and Part D non-interference statutory frameworks.[12]

Health plans already provide web-based platforms or apps that contain price estimates with other helpful information such as quality metrics. Only health plan tools can provide consumers with accurate, personalized, meaningful information such as whether a service is covered and where they are in their deductible. Policies, like the Transparency in Coverage rule (TiC), that require publicly sharing large data sets containing confidentially-negotiated rates have not provided actionable information to consumers. The TiC machine-readable files to date have been used for business intelligence, not consumer purposes or even research.

Should HHS seek other ways to share data with third parties to develop into information for consumers, this can be done without disclosing contracted information or trade secrets. For example, providing cost tiers or the relative costliness of a provider compared to others. Or, providing composite value scores comprised of cost, quality, and patient experience information, where the negotiated amount cannot be backed into like co-insurance.

HHS should not seek additional disclosures of confidentially negotiated rates, but rather assist health plans in educating consumers about the availability of plan cost calculator tools to increase their usage.

Improve Quality Information

We support the government's vision to leverage HIT to make information about quality more accessible to consumers and alleviate the burden of measurement on payers and providers. Information on quality is an essential complement to information on costs and pricing. Quality measures allow consumers to understand the value offered by a provider relative to others and can serve as important protections against stinting of care, especially for patients who are members of racial or ethnic minority groups who may experience access challenges that can skew cost data in the absence of information about quality.

---

[11] Koslov, T. and Jex, E.; *Price transparency or TMI?;* Federal Trade Commission Blog; Jul 2, 2015 2:31PM; https://www.ftc.gov/news-events/blogs/competition-matters/2015/07/price-transparency-or-tmi.
[12] 42 U.S.C. 1395w-111(i); 42 U.S.C. 1395w–24(a)(6)(b)(iii).

Objective D: Providers experience reduced regulatory and administrative burden.

Leverage Electronic Prior Authorization

We appreciate the federal government's efforts to reduce the administrative burden and agree technology will play an important role in streamlining processes and enhancing efficiency. We agree that electronic prior authorization has great potential to reduce the burden of the prior authorization process while maintaining an important safety and quality check. For example, we have broadly supported CMS's vision in the *Interoperability and Prior Authorization* final rule and are focused on implementing its policies successfully. **We urge the government to support the necessary infrastructure to implement the APIs outlined in the final rule, including the NDH as a directory resource, and mature and sufficiently tested standards and IGs. Electronic health record vendors should be required to build and health care providers must use the electronic prior authorization APIs offered by health plans**

Reduce Quality Measurement Burden

Technology holds promise to further reduce the administrative burden by reducing the data collection efforts required to report quality data. Digital measures and the electronic exchange of information through formats such as APIs could reduce the time and resources required to extract data from patient charts, surveys or other forms used to generate patient-reported outcome measures. Moreover, digital quality measurement (dQM) could allow novel concepts that could not previously be assessed due to data limitations.

Ongoing work by HL-7 such as the C-CDA and DaVinci Implementation Guides can lay the groundwork for better exchange of the data needed to support digital measurement. However, the necessary standards and implementation guides must be sufficiently tested and mature before widespread implementation is possible. Testing and maturity of the standards will be essential to the scalability and feasibility of digital quality measurement.

ONC and CMS must also require all stakeholders involved in the measurement enterprise to build the necessary connections and share the necessary data to support dQMs. ONC should work with CMS to ensure certified EHR vendors build the data elements required for dQMs into their products. ONC and CMS should also require providers to share data with health plans electronically to ensure feasibility and alignment across payers. Using technology in this fashion will reduce provider burden while simultaneously creating information on provider value for consumers, payers, and purchasers.

We also encourage CMS to foster alignment on the adoption and approach to digital quality measurement across the industry. CMS should work with NCQA and other measure developers to ensure synergistic approaches to adopting FHIR resources. CMS should also work with the CQMC and health plans to advance alignment of the use of dQMs across public and private payers.

Promote Safe and Responsible Use of AI

As noted above we support efforts to promote the safe and responsible use of AI. AI offers great potential to improve care delivery. We agree with ONC's approach in the HTI-1 rule to focus on promoting transparency rather than outside reviews of AI tools. Successful use of AI to enhance high-quality, equitable, and affordable care will depend on responsible, risk-based approaches to both AI development and AI deployment. In the current environment, there are no established standards for delineating roles and responsibilities across the AI ecosystem, including between AI "developers" and "deployers," if an adverse outcome occurs from the use of AI.

Currently, there is also a lack of broadly applicable, established standards for transparency or disclosure of key elements of AI tools sold by vendors that would enable deployers to proactively assess the potential risk of errors, safety hazards, or discrimination, including to support evaluation efforts during the initial procurement phase of adopting new AI technology. Of particular concern are the Generative AI (GenAI) models that, for example, develop new content, images, video, and audio. These GenAI models are trained on massive amounts of data and generally offer little transparency into the datasets used to train the models and other key components of the model's design that could contribute to promoting bias. In addition, the use of Deep Neural Networks (DNN) within Machine Learning is concerning because even the developer may not be able to explain the way in which the AI-derived the results. AI developers should share relevant details with purchasers of high-risk AI to inform efforts to identify and manage risk while optimizing safety and effectiveness.

For AI tools developed internally, health care organizations should be able to leverage existing, robust testing, monitoring, and data governance processes. AHIP does not recommend requiring the disclosure of proprietary information related to internally developed tools by health care organizations, as they are already subject to extensive legislative and regulatory privacy, security, and consumer protections not requiring third-party evaluation, audits, or transparency of proprietary information.

AHIP has concerns that a strict definition of accountability could cause undue burden and restrict innovation as technology keeps advancing. **We recommend that the federal government look to established national frameworks, engage trusted federal partners and standards development organizations, and leverage learnings from public-private efforts to inform any legislative policy efforts that address risk-based accountability in AI use.**

Goal 3: Accelerate Research and Innovation

Objective B: Individual and population-level research and analysis are enhanced by health IT

We support ONC's vision to enhance research are care delivery through better data and improved access to technology. We also appreciate the agency's commitment to balancing this goal with protecting patient privacy and preventing unintended harms. For example, as noted above, we strongly support this objective including a strategy to "Protect de-identified health information from re-identification." As big data becomes more available and interest in developing

technologies such as AI grows, it is essential that patients' private health information is robustly protected by all parties who may have access to it.

As noted above, apps may not be covered by HIPAA and can sell or re-use a person's data without authorization beyond the initial check box terms of service. Many consumers may not thoroughly read the terms and conditions of an app's use or fully understand the implications of sharing their data outside of HIPAA. Even those who do often only have the choice of either agreeing to the terms or not using the service. As the information changes hands down a chain of entities, the privacy and security of the information become increasingly vulnerable risking inappropriate disclosure and re-identification of other data sources. Research has found that de-identified data can be accurately re-identified by correlating several data points such as a person's date of birth, zip code, and gender, potentially exposing a person's identity and medical history.[13,14] Re-identification research has found that the more data points available to support re-identification, the greater the likelihood of an accurate match. One study found that 15 demographic data points could correctly re-identify more than 99% of Americans.[15]

elements should be used to improve the health and well-being of consumers and weighed against the risks associated with its disclosure. ONC should reconsider the inclusion of individually identifying data elements in the Health Insurance Information data class, like Member Identifier or Subscriber Identifier that are not necessary to support functions like user authentication for apps. Health care and health plans have established alternative secure user identification protocols for authorized users to obtain data. Moreover, this granular level of detail poses a real threat to consumers if obtained by bad actors.

<u>Objective C: Researchers advance health equity by using health data that includes underrepresented groups.</u>

Underrepresentation of certain demographic groups in the underlying data used to support technologies such as AI, ML, and advanced analytics is a problem. Stakeholders, including researchers and health plans are taking decisive actions to improve the completeness of the demographic data that underlies such tools to better understand potential biases. Improving demographic data standards and collection will allow AI developers to build tools that benefit more people and mitigate adverse bias that can result from not representing all populations in the data used to build and train AI solutions. However, it will take time to build these more robust data sets.

While we work collectively to improve the underlying data and better understand potential sources of adverse bias in technologies like AI, mitigation will be key. However, it is difficult to define remediation standards when there is not yet a standard on when adverse bias is occurring and if it requires mitigation. For high-risk technology products and services leveraging technologies such as AI, there is a need for greater transparency on how AI is built and what underlying data sets have been used to train it. While we appreciate the need to protect intellectual property, we support risk-based approaches to transparency, such as the intent of

---

[13] https://www.theregister.com/2021/09/16/anonymising_data_feature/
[14] https://georgetownlawtechreview.org/re-identification-of-anonymized-data/GLTR-04-2017/
[15] https://www.nature.com/articles/s41467-019-10933-3?source=techstories.org

ONC's new DSI criteria in the Certification Program that focus on providing end users with the information they need to better understand how an AI is built and what mitigation approaches may be necessary to protect against bias.

We look forward to working with ONC and other government agencies to address these issues. AHIP believes public-private partnerships and collaboration can play an important role in facilitating data-driven efforts to address adverse bias in AI. For example, in December 2023, the Agency for Healthcare Research and Quality (AHRQ) published a paper titled "Guiding Principles to Address the Impact of Algorithm Bias on Racial and Ethnic Disparities in Health and Healthcare."[16] The guiding principles outlined in the report were developed following a government-sponsored convening of experts from across the healthcare ecosystem, including health plan representatives.

Industry standards are needed on how to identify bias, as well as when and how to remediate it. **We also look forward to working with ONC to define algorithmic bias and develop standards against which to measure adverse bias and take action to minimize it.**

Goal 4: Connect the Health System with Health Data

Objective A: Development and use of health IT capabilities continues to advance.

We support the inclusion of a strategy to "collaborate across public and private sectors on health IT standards' maturity, adoption, and use." Mature and tested standards and IGs are essential to the success of policies such as the APIs mandated in the CMS interoperability rules. Given the development and maintenance of standards and IGs are an extension of federal policy that does not go through the rulemaking process, it is critical that this development and maintenance process be consensus-based, fair, transparent, and open to all stakeholders. And, that policy decisions are not delegated to this process, but rather through formal agency mechanisms. For example, the IG creation process is currently driven by a limited number of volunteers that do not broadly represent the industry, which results in creates IG Resource/Profile versioning issues. Ensuring there is no fee to fully participate in the process for the regulatorily required exchanges and relying on an ANSI accredited process to develop the IGs would improve the approach. Content and technical standards as well as IGs must be fully developed and sufficiently tested for successful implementation of truly interoperable sharing and transparency. Mature standards, as well as sufficient timing to adopt, should be a precursor to implementation. The standards development process should not be used as a means to refine policy requirements. Where possible, existing Standards Development Organizations recognized under HIPAA and other federal laws should be utilized as part of the overall plan.

---

[16]https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2812958?utm_source=For_The_Media&utm_medium=referral&utm_campaign=ftm_links&utm_term=121523

Objective B: Health IT users have clear and shared expectations for data sharing

Promote information sharing practices

We appreciate CMS's and ONC's efforts to date to promote interoperability and increase information sharing. As the federal government develops plans to promote the flow of information, we urge the implementation of policies that allow all relevant stakeholders to receive information. As noted above, CMS and ONC should make the Provider Access API bidirectional to allow health care providers to share data with health plans. ONC should also leverage the Certification Program to require EHR vendors to build the necessary connections to promote the CMS APIs, especially the Prior Authorization API to ensure providers can implement this technology. Finally, CMS should consider broader and more meaningful incentives for providers to use the Prior Authorization API.

Advance a Trusted Exchange Framework and Common Agreement (TEFCA)

AHIP appreciates ONC's efforts to launch TEFCA to promote information sharing. However, the use cases supported by TEFCA must appeal to a broad range of entities including not only health care providers, but also health plans, public health agencies, consumers, clearinghouses, and other integral entities to fully meet its potential. We urge ONC and its Recognized Coordinating Entity (RCE) to bring health plans more fulsomely into the process as central stakeholders in the development and use of TEFCA. Additional health plan representatives should be included in TEFCA advisory groups and plan representatives should be considered for chair roles. **Moreover, these representatives should come directly from health insurance companies or their trade associations rather than vendors who cannot accurately speak to the needs of health plans**.

Education, incentives, and equitable engagement are necessary to support sufficient participation in this network. ONC and the RCE should consider opportunities to support connectivity, including technical and financial assistance, for providers that were historically left out of health IT adoption programs and may have limited adoption of FHIR capabilities at this time.

Additionally, TEFCA should pursue use cases that benefit all health stakeholders and incentivize use including use cases that allow health plans to fully participate in the exchange such as supporting the CMS APIs and non-treatment exchange. Initial recommendations include ADT information, electronic prior authorization (ePA), and data needs for quality programs. ONC should also explore ways to support implementation of FHIR API technology to facilitate trust in the exchange. **We recommend the RCE work with health plans and stakeholders to discuss opportunities to increase TEFCA participation.**

Objective D: Individuals' EHI is protected, private, and secure.

Allow Individuals to Understand and Control Use of their EHI.

Protecting members' health data is paramount to health plans. As noted above, we strongly support efforts to address the threats to patient privacy introduced by third-party apps that are not

covered by existing laws and regulations. We also support efforts to educate patients on the risks of data sharing and believe the federal government should take the lead on these efforts, including by providing educational resources health plans and providers can share with patients. We also support efforts to enhance transparency about potential secondary uses of data and the risk that this can pose so patients can make informed choices about how and with whom to share their data.

Integrate High-Impact Cybersecurity Practices

As a critical infrastructure sector, health care organizations are under persistent attack by cyber criminals, including nation-state actors. In 2023 alone, there were over 460 ransomware incidents affecting the U.S. health sector.[17] Underscoring the severity of the threat landscape, the number of breached health care records increased by 156% from 2022 to more than 133 million records in 2023.[18]

Given the scale and scope of the ongoing cyberattacks, we fully agree that stakeholders and policymakers must work together in public-private partnership across the federal government, states, and the health care system to better protect Americans going forward. The February 21, 2024, cyberattack against Change Healthcare reinforced the interconnectedness of the health system and the importance of robust cybersecurity emergency preparedness and resilience planning. It is vital that all stakeholders – health plans, physicians, facilities, pharmacies, and others – adapt, prepare, and invest in the capabilities to minimize disruptions in the first place

AHIP supports a comprehensive approach to cybersecurity. This includes collaboration with private sector stakeholders and coordination across federal government agencies in the education, emergency preparedness planning, mitigation, and response phases of a cybersecurity incident and ensuring no one is left behind in cybersecurity efforts. This can include the need for federal health care programs to provide emergency relief and authority for extensions and adjustments to timelines for statutory and regulatory measurement and reporting requirements. Waiver authority is often used to provide flexibilities in public health and other emergency situations.

AHIP is an active member of the Health Care and Public Health Sector Coordinating Council's Cyber Working Group (CWG). The mission of the CWG is to collaborate with HHS and other federal agencies to identify and mitigate systemic risks that affect patient safety, security, and privacy, and consequently, national confidence in the health care system. Through the CWG, AHIP engages in key initiatives to ensure the health care sector at large has access to resources and best practices and opportunities to engage with key decision makers from across the federal government.

As covered entities under HIPAA, health plans are subject to the requirements of the HIPAA Privacy and Security Rules, including stringent breach notification requirements. HIPAA has robust security standards that OCR vigorously enforces. **However, the Change Healthcare**

---

[17] http://www.hhs.gov/sites/default/files/ransomware-healthcare.pdf

[18] https://www.hipaajournal.com/security-breaches-in-healthcare/#:~:text=2023%20was%20the%20worst%2Dever,records%20were%20breached%20every%20day

attack has shown we must all come together to protect the health care system from future attacks and ensure resiliency when attacks do happen. For example, Congress could consider legislation that would permit CMS and other agencies to temporarily waive statutory requirements to ensure that sufficient health care items and services are available to meet the needs of affected patients during large-scale cybersecurity events. Congress should consider potential policies to support smaller and less well-resourced providers and health delivery systems in efforts to ensure robust protections and planning. Potential options include federal funding for cybersecurity capabilities, the replacement of obsolete technologies, and promoting additional education, awareness,
and continuity planning.