America's Health Insurance Plans
601 Pennsylvania Avenue, NW
South Building, Suite Five Hundred
Washington, DC 20004

Matthew Eyles
President and CEO

June 3, 2019

Seema Verma
Administrator
Centers for Medicare and Medicaid Services
Department of Health and Human Services
Attention: CMS-9115-P
P.O. Box 8016
Baltimore, MD 21244-8016

Submitted electronically via www.regulations.gov

RE: [CMS-9115-P]: Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Interoperability and Patient Access for Medicare Advantage Organization and Medicaid Managed Care Plans, State Medicaid Agencies, CHIP Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans in the Federally-Facilitated Exchanges and Health Care Providers

Dear Administrator Verma:

On behalf of America's Health Insurance Plans (AHIP), thank you for the opportunity to offer comments in response to the Centers for Medicare & Medicaid Services' (CMS) proposed rule on Interoperability and Patient Access published in the *Federal Register* on March 4, 2019 (CMS-9115-P).

AHIP is the national association whose members provide coverage for health care and related services to millions of Americans every day. Through these offerings, we improve and protect the health and financial security of consumers, families, businesses, communities, and the nation. We are committed to market-based solutions and public-private partnerships that improve affordability, value, access, and well-being for consumers. We applaud the Department of Health and Human Services' (Department's) continued efforts to promote transparency and accessibility of health information to support consumers in health care decision-making. Health insurance providers are committed to finding innovative ways to integrate and share data with consumers, doctors and hospitals. Improving access to meaningful information can help all actors in the health care ecosystem to realize the full benefits of health information technology and data sharing—from improving care coordination to providing access to patient out-of-pocket cost and quality information—to achieving better health outcomes, more affordable care, and higher patient satisfaction.

AHIP and our members share the Administration's goal of providing patients access to their health information to promote better choices about care and treatment. We also agree that health insurance providers have a critical role to play in consumer access to and the interoperability of health information. Most plans currently use web-based technologies to provide enrollees with user-friendly information on their care, its costs, and indicators of provider value.

In reviewing this rule, we focused our comments on ensuring that consumers get the information they need when and where they need it. However, transparency and access must be balanced with the need to maintain patient protections, minimize administrative burdens on all stakeholders, and establish and adopt clear data standards and operational protocols to put meaningful information into the hands of patients, doctors, and health insurance providers.

While we support the Department's efforts, AHIP and our member companies have concerns that focus in four areas:

- the unrealistic 2020 effective date being proposed,
- the lack of mature standards for the proposed data elements and exchange,
- the absence of privacy and security protections for patient data accessed through third-party applications ("apps"), and
- the possible release of granular price information that could result in increased costs for consumers and cause other anti-competitive consequences.

Our comments and recommendations regarding the proposed rule reflect AHIP's commitment to continue our partnership with the Administration to develop policy solutions that will support a more consumer-focused market, ensure access to meaningful, actionable information, and promote quality and affordability. **AHIP and its members look forward to a public-private partnership across a multitude of stakeholders to make true interoperability of health information a reality.** Below we summarize AHIP's comments and recommendations on key issues. A more detailed compilation of our comments is included in the attached Appendix:

Patient Privacy Is Paramount. As written, the proposed rule includes no certification process for third party applications ("apps"). Given the access to personal health information these apps are expected to have, we recommend that a process be established by the Federal Trade Commission (FTC), in partnership with the Department under which apps are vetted for the adequacy of the consumer disclosures, as well as the privacy and security of the information once it is no longer governed by the Health Insurance Portability and Accountability Act (HIPAA) and secondary uses are permitted. While CMS and others draw the parallel to use of third-party apps to conduct personal banking, the implications and consequences of a potentially widespread availability of personal health information are arguably far greater. If the Administration determines it does not possess sufficient authority to create a robust oversight and enforcement framework for these apps it should ask Congress to extend its authority. Consumers need confidence that this sensitive information is being treated with care and integrity to encourage widespread use of these apps.

Consumer Education Will be Essential to Protect Privacy. All stakeholders should play a role in patient education regarding data sharing. At the same time, we believe the Department in collaboration 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 and how to lodge complaints against them. Given CMS' experience implementing the Medicare Blue Button 2.0 initiative as well as the associated consumer education campaign, CMS is well situated to leverage lessons learned and apply them to this broader consumer education efforts.

Model consumer notifications and educational materials should be developed and made available for insurance and healthcare providers to use voluntarily. Education should clearly advise consumers that HIPAA protections do not apply and that the insurance or healthcare provider furnishing the data on their behalf are not responsible for the privacy or security of the data obtained by apps or sold for secondary uses.

Implementation Timeline Should be Phased-In No Sooner Than 2022 and Tied to Development of Standards as well as Consumer Privacy Protections. While health insurance providers embrace the movement toward seamless exchange of consumer data, we have significant concerns that the proposed implementation timeline fails to recognize both the operational complexity associated with building the required technology and the lack of mature standards for the proposed data elements and exchange. For example, while claims information already uses HIPAA standards for the transmission of information, comparable Fast Healthcare Interoperability Resources (FHIR) standards are not yet available. Additional operational parameters are also necessary, thus implementation of the requirement to participate in a Trusted Exchange should be staged to coincide with the finalization of the Trusted Exchange Framework and Common Agreement rules. In addition, patient matching rules will be critical to the proposed coordination of care policies where the consumer may no longer have credentials to electronically access their health information from their former health insurance provider. However, this issue is still in the "request for information" stage.

Furthermore, implementation needs to account for the different program contracting cycles to allow for time to factor in additional costs associated with the new requirements. The proposed effective dates—between January 1, 2020, and July 1, 2020 (depending on plan type)—are not feasible. In addition to posing significant compliance burdens not only on health insurers, providers and other stakeholders in the health care system, the timing risks undermining the effectiveness of this effort which all stakeholders want to be successful. With respect to Medicaid programs, we recommend that CMS allow a longer period for implementation based on the full implementation of the Transformed Medicaid Statistical Information System (T-MSIS) and align Medicaid Managed Care Organizations with that timeline. CMS should also immediately develop a voluntary, multi-payer pilot project to test the sharing of health information via APIs. This pilot, which could be conducted in 2020, would then inform national implementation as standards mature.

Lastly, as discussed above, education of consumers and oversight of the third-party apps is a foundational step that must be taken in advance of implementation.

Inclusion of Granular Price Information in the Scope of the Data Could Have Unintended and Anti-Competitive Consequences. The proposed scope of the data required to be shared by health insurance providers with patients via third-party apps includes claims data with provider level payment information. AHIP and our members are firmly committed to providing consumers greater price transparency to aid in their decision-making and empowering them to choose health care services that are both affordable and right for them. Health insurance providers offer transparency tools that give consumers estimates of anticipated costs and ways to compare services based on price, quality, and accessibility. As CMS develops its final rule, we urge consideration of the unintended consequences of the release of granular pricing data on the progress private-sector health insurance providers have already made to provide tools and convey useful information to consumers.

Much of the information included in claims are not useful or relevant to consumers. In addition, trying to fully adapt these comprehensive administrative transactions to a consumer-friendly API-based format will slow down the standards development process. CMS should focus on the most relevant information to the consumers in the claims. Moreover, requiring public disclosure of pricing data could have potentially negative competitive effects that could hinder fair negotiations and drive up prices. According to 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."[1] Should disclosure of private contract negotiations be required, the cost impacts could be significant, causing serious disruption to our health care system to the detriment of consumers. **CMS should begin with what is most useful to patients and only require the exchange once the relevant FHIR-based standards are established. This should not include negotiated rates or any other information that could reveal trade secrets.**

AHIP and its members are committed to working with the Administration and other stakeholders to advance greater interoperability and patient access to and control over their health information, with the ultimate goal of improving the quality and affordability of the care they receive. Along with our members, we thank you for allowing us to comment and look forward to a robust and collaborative process to bring this bold vision to reality. If you have any questions, please reach out to Danielle Lloyd, senior vice president for private market innovations and quality initiatives at either dlloyd@ahip.org or 202-778-3246.

Sincerely,

Matthew Eyles

Matthew Eyles
President and CEO

[1] 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.

Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Interoperability and Patient Access for Medicare Advantage Organization and Medicaid Managed Care Plans, State Medicaid Agencies, CHIP Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans in the Federally-Facilitated Exchanges and Health Care Providers

AHIP Detailed Comments

I.A. CHALLENGES AND BARRIERS TO INTEROPERABILITY

The Centers for Medicare & Medicaid Services (CMS) outlines what it sees as the primary challenges and barriers to providing patients with access to their health information including:

- Patient Identifier and Interoperability,
- Lack of Standardization,
- Information Blocking,
- Lack of Adoption/Use of Certified Health IT Among Post-Acute Care (PAC) Providers, and
- Privacy Concerns and Health Insurance Portability and Accountability Act (HIPAA).

We concur with CMS that each of these are indeed barriers to interoperability and appreciate that CMS and the Office of the National Coordinator for Health Information Technology (ONC) are working in tandem to overcome these challenges with stakeholder input and participation. **One challenge that is not highlighted in the rule is the insufficiency of the tech industry resources needed to move the majority of insurance and healthcare providers to standardized web-based technologies in such a short timeframe.** As we proceed, it is important to note that the stakeholders and resources required to mitigate each barrier differs. Each requires unique strategies and tailored timelines by use case. For example, the conflicting web of state privacy laws cannot be immediately addressed and thus requires accommodation. Standards setting bodies are working feverishly to create mature industry-wide standards across a wide range of use cases so that everyone can use application programming interface (APIs) to exchange the information needed to achieve each specific goal. However, each standard will mature at a different rate requiring transition over time. As we discuss the proposed policies below, we will embed suggestions on exceptions and how to stage the proposals as well as collaborate with industry stakeholders to successfully surmount the hurdles ahead of all of us to achieve our common goal of empowering consumers with their health information while minimizing potential unintended negative consequences.

Industry-CMS Working Group

We believe it would facilitate implementation if CMS convened a group of 10-12 subject matter experts from health insurance providers along with other relevant stakeholders, such as developers, to meet with CMS, ONC, and FTC to facilitate a smooth path to the application programing interface (API) compliance deadline and ensure a successful implementation. The scope for this workgroup should include payer-to-payer and payer-to-consumer data exchange. Industry representatives would work collaboratively with each other and CMS to identify sources of confusion, outstanding policy, operations, and technical questions that must be addressed prior to implementation. This working group would share an industry perspective and provide informal input to CMS on a broad range of

implementation and compliance issues. For example, issuers may provide insight on success in meeting development milestones, areas in which additional CMS guidance is needed, testing processes and timeframes, developing robust consumer communications and education, unforeseen barriers, and providing an overall industry perspective on readiness of API technology to provide accurate, meaningful information to consumers. We recommend this group convene on a regular basis, at least twice monthly, leading up to and after the compliance date to continually address issues related to access of health data through APIs. The group could also advise CMS on the implementation of any pilot projects as discussed later in our letter. **CMS should engage an industry working group to work collaboratively in a public-private partnership with CMS to overcome the outlined challenges and ensure successful implementation of API technology.**

III. PATIENT ACCESS THROUGH OPEN API

III.B.1. Benefits of Information Access

We agree with CMS that there are many benefits associated with individuals having simple and easy access to their health care data. Health insurance providers do this today by making claims information available to members in digital formats along with tools to estimate the cost and quality of potential hospital or physician services in their web-based technologies. We recognize that giving members access to the clinical information contained in electronic health records (EHRs) held by providers would provide them with a more holistic view of their care. We further agree that to accomplish true interoperability across stakeholders in an efficient and comprehensible way, additional data content and exchange standards are needed. This will permit not only exchange with consumers, but also among payers, providers and others such as application (or "app") developers to improve the experience, quality, coordination and efficiency of care. However, the proposal also raises significant privacy risks to enrollees given the unique nature of personal health information (PHI) and that it will no longer be subject to Health Insurance Portability and Accountability Act (HIPAA) protections. **As we contemplate the evolution to the desired state of wide-spread health care data interoperability, we need to consider what problems we are trying to solve for the consumer (the use cases), what information is necessary to do so (content standards), and then how to best share that information (technical standards) in order to strike a balance between risks and benefits.**

While there are clearly benefits to facilitating data access, we must also weigh the risks to determine the best path and appropriate timing to achieve the goal without creating new consumer challenges. Recent research[2,3,4,5,6] shows that third-party health apps pose unprecedented risk to consumers' privacy given their ability to collect user data that is highly valuable to commercial interests as well as their ability to re-identify consumers in other de-identified datasets.

---

[2] https://www.sciencedaily.com/releases/2019/03/190321092207.htm
[3] https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636;
[4] https://www.wsj.com/articles/popular-apps-cease-sharing-data-with-facebook-11551044791
[5] https://www.washingtonpost.com/business/2019/04/22/smoking-depression-apps-are-selling-your-data-google-facebook-study-finds/
[6] https://www.wsj.com/articles/popular-apps-cease-sharing-data-with-facebook-11551044791

Health care is not like banking. While one can open a new bank account after fraud, one cannot expunge public awareness of personal or familial health history. While patients may not understand the intricacies of HIPAA, patients have a general sense that they have privacy rights when it comes to their health information and that its protection is held to a high standard. It is not clear how quickly that social understanding will adapt as an unprecedented amount of potentially sensitive information is beyond the reach of HIPAA. Without comparable privacy and security standards applied to the third-party developers, the same information guarded so carefully by covered entities will be readily made available for purchase. AHIP and its members are concerned that sharing copious amounts of PHI too quickly (even if legally) and without sufficient protections will have unintended consequences for consumers. For example, they may unwittingly accept terms and conditions permitting secondary uses of their data, especially if the detailed and technical nature of those terms and conditions prevent them from being fully informed of the potential risks they face. The greater the volume of data, the greater the likelihood information will be misused or shared in ways in which patients are unaware and/or are uncomfortable.

Beyond privacy concerns there are also increased data and national security risks. Rushed implementation could compromise the necessary testing and refinement of the open APIs. Moreover, the greater the scope of data and number of parties holding the data will create more opportunity for unscrupulous actors to make attempts to illegally obtain the data.[7] It is not far-fetched to imagine foreign states or organized crime syndicates seeking information at either a personal or population level to facilitate illegal activities. While these examples may seem extreme, the state of internet vulnerabilities tells us that such schemes are possible, and we have to do our best to anticipate and plan for such events.

We urge CMS to start with a small subset of volunteer health insurance providers and expand deliberately over time to minimize the risks and possible public backlash that could undermine the ultimate goal of interoperability. We urge CMS to stage implementation based on the content most important to consumers, the maturity of standards, the development of an app certification program and exclusions process, and sufficient time for health insurance providers to test, deploy, refine and safely scale.

III.B.2. Alignment with HIPAA

As noted by CMS, patients have the right to access their PHI and direct that it be shared with a third-party. In addition, a covered entity cannot deny such a request based on concerns about the worthiness of the third party as a recipient of PHI or what it might do with the PHI. Despite the fact that the law does not dictate the information must be provided through an API, we agree that in the digital age patients should be able request that their health insurance provider share PHI with an app of their choosing. We furthermore agree with CMS that the health insurance provider requirements should fall within the HIPAA Privacy and Security definitions and provisions. The proposals create a new pathway for health insurance providers to meet existing data access and sharing requirements. However, we note that in response to the February 2019 request for information (RFI) from the Office of Civil Rights (OCR), we provided several suggested potential revisions to HIPAA policies.

[7] http://homepage.divms.uiowa.edu/~sfarooqi/Files/Farooqi-AbusiveTwitterApplications.pdf

We indicated support for OCR's desire to evaluate potential revisions to provisions of the existing HIPAA regulations that may impede the ongoing transformation to value-based care or interfere with coordinated care without meaningfully protecting the privacy or security of PHI. **The Department should ensure that future proposed changes under HIPAA consider and incorporate the polices contained in this rule. Furthermore, CMS should ensure that its finalized policies fall within the requirements of HIPAA and rely on the related definitions and policies to help ensure clarity and consistency and build on the existing infrastructure and experience with HIPAA compliance.**

As described in recent OCR guidance, the HIPAA privacy and security regulations permit covered entities to deny access to apps that it has legitimate concerns will pose a threat to their own system. This is critical to ensuring the security of not just the requesting patient's PHI, but also that of all enrollees. **We believe the Department should make it clear that this guidance enables health insurance providers to delay and/or deny access to certain apps that are suspected of or proven to be bad actors.**

This is especially true as we expect to encounter app developers that are neither covered by HIPAA nor the Federal Trade Commission's (FTC) regulatory requirements for electronic health vendors, and thus currently have few restrictions on their actions and little oversight. The FTC does have authority under the FTC Act to investigate unfair or deceptive trade practices, along with certain breach provisions, but the FTC will need to establish an additional policy and enforcement framework for this new area beyond the developer guidance that exists today in order to truly protect consumers. Moreover, it is likely that the FTC will need additional authority to ensure the privacy and security of the data that was formerly PHI. For example, it does not have the authority to require apps meet basic data security standards. Comprehensive oversight and enforcement by the FTC is paramount to patient's trusting the apps and being willing to share their data. **Implementation of open payer-to-consumer APIs should not be required before the FTC is able to develop a privacy and security oversight and enforcement framework for health apps accessing PHI from insurance and healthcare providers building off the HIPAA privacy and security regulations where it can and seeking additional authority where necessary.**

We recognize that covered entities are not responsible or liable for the privacy or security of PHI once it is received, maintained, used or redisclosed by an app chosen by an individual. Likewise, it is not the responsibility of a covered entity when certain non-HIPAA-covered entities disclose an individual's health information in a manner that is not consistent with the privacy notice and terms of use to which the individual agreed. However, patients will not readily understand the line between HIPAA-covered entities and non-HIPAA-covered entities including the difference in permitted uses and security safeguards. While we are hopeful that the educational efforts of the Department, FTC, apps as well as insurance and healthcare providers will help to elucidate these differences for consumers to enable informed consent, we continue to fear that a lack of understanding will create reputational risks for health insurance providers who are simply complying with the law. **CMS should make it starkly clear in its final regulations via a safe-harbor provision in the regulatory text for covered programs that insurance and health care providers are not responsible for the**

downstream privacy and security of the PHI shared with patient-selected apps consistent with the recent guidance issued by OCR.[8]

III.C. OPEN API

CMS's proposed policy would apply to Medicare Advantage (MA) organizations, state Medicaid and CHIP fee for service (FFS) programs, Medicaid managed care plans, Children's Health Insurance Program (CHIP) managed care entities, and qualified health plan (QHP) issuers in federally-facilitated exchanges (FFEs). Specifically, these entities would be required to implement, test, and monitor a transparent and standardized web-based technology to make patient claims and other health related information available electronically, at the request of the patient, to all secure application developers. CMS seeks to standardize not only the content shared, but also the technology through which it is shared to speed the ability of the technology sector to harness the data.

III.C.2. b. API Technical Standard

Applicable entities would be required to implement, test, and monitor an openly published Fast Healthcare Interoperability Resources (FHIR)-based Application Program Interface (API) to make patient claims and other health related information available electronically, at the request of the patient, to all secure application developers. Furthermore, complementary security and app registration protocols would be required using either OAuth 2.0 or OpenID Connect Core. **AHIP and its members support the proposed technical standards but suggest that CMS clearly define in the regulations that an open API means one that is based on openly-published standards that are not proprietary.**

We agree with CMS that it is beneficial to generally harmonize the plan and provider required standards in the CMS and ONC proposed rules. There is a tension, however, between the need to coalesce around a specific standard to efficiently and quickly move the industry forward and the inability of the regulatory process to keep up with the pace of technological advancements. While there is a strong argument for codifying not only a specific standard but a specific version of that standard so that the industry commonly builds from the same starting point, the reality is that the favored standard will change over time and the pace at which each organization can evolve to the next standard will vary. **To balance this tension, CMS should codify via cross reference the relevant API standards endorsed by ONC as a floor, not a ceiling, and allow for updates via the ONC Standards Version Advancement Process with adequate public input and time for implementation.**

We greatly appreciate that CMS intends to provide technical assistance throughout implementation of these policies. Given its experience in building the Blue Button 2.0 initiative, we anticipate there were many lessons learned that would be beneficial to share with the health insurance providers and states subject to these policies to reduce the time and resources necessary to build the technology and surrounding operating protocols. For example, health insurance providers would benefit from the

[8] https://www.Department.gov/hipaa/for-professionals/faq/3009/does-a-hipaa-covered-entity-bear-liability.html

preparation and release of implementation guides. We caution CMS, however, not to use implementation guides to fill gaps in inadequate or immature standards. **CMS should stagger implementation by use case as standards mature and are thoroughly tested.** In addition, it may also be helpful for those health insurance providers and states that do not currently maintain any APIs for CMS to provide the underlying code for a compliant API. **CMS should make available implementation guides and other tools sufficiently in advance of the required implementation date to facilitate the development and testing of health insurance providers and states capabilities.**

III.C.2.c. Content and Data Standards

The categories of data CMS proposes to require via the open API include adjudicated claims data, including provider remittances and beneficiary or enrollee cost-sharing data, encounters from capitated providers, provider directory and clinical data, including laboratory results managed by the payer.

III.C.2.c(1) Patient Claims and Encounter Data

The proposed required content includes information plans have available electronically through the HIPAA-named transaction set standards— X12 837 – Claim Submission and 835 – Claim Payment/Remittance Advise. CMS specifies that adjudicated claims data includes approved and denied claims. CMS also requires payers make this data available no later than one business day after the claim is processed or the encounter data record is received.

Standard

Health insurance providers use the HIPAA-named transaction set standards to easily communicate with providers to confirm coverage eligibility, share benefit structures, make payments etc. However, API-enabled FHIR-based standards that would allow for the seamless exchange of such information from health insurance providers to consumers and third-party apps is still being developed. Developing and testing these standards will be more complex than it might seem despite existing HIPAA and clinical standards. For example, elements such as diagnosis codes have been standardized for decades, most recently to the ICD-10 standard. Mapping these within a dataset is relatively straight forward. Denial codes vary by plan, both in how they are defined and how they affect the logic of each plans' payments and claims administration. Even with standardized data elements, extensive testing is required to ensure a standard is suitable for a given purpose. For example, without considering the impact of coordination of benefits between payers and subrogation, the dataset might give a misleading or incomprehensible result. So, while ICD-10, and other clinical data elements, are common universally adopted languages, elements of the claims adjudication process have separate payer-specific languages, each with its own vocabulary and grammar. Translating and interpreting these languages through the API, without losing or confusing the payer's meaning is challenging. That work is underway and progressing quickly. Relying on immature standards will result in consumer confusion or worse. **Implementing the API requirements by use case in phases as standards are mature will ensure smooth adoption of APIs. Moreover, the Department has not finalized standards for claims attachments and thus should not require**

their inclusion. CMS should continue its public-private partnership with the HL7 DaVinci Project and other industry groups, such as the CARIN Alliance, to establish FHIR-based technical standards for a subset of data elements in the claim forms for which there is a patient-centric use case as a first step in implementing the proposed policies.

API Content

CMS notes that the content shared through the API should be comparable to the HIPAA-named transaction set standards— X12 835 and 837. In Listening Sessions, CMS presenters suggested that the information commonly found on Explanation of Benefits (EOB) forms would be expected rather than the full claim. If we consider the patient-centric use case and borrow the notion of the minimum necessary information, CMS should require a discrete subset of claims information. We agree that the initial data elements surfaced should be comparable to an EOB as much of the information included in these transactions are not useful or relevant to enrollees and would rely heavily on a developer's impossibly granular understanding of the specific insurance policy and issuers' system logic to avoid creating confusion or misinformation. In addition, trying to fully adapt these comprehensive transactions to a consumer-friendly API-based format will slow down the standards development process. **CMS should focus on the most relevant information to the consumers in the claims and require implementation only once the relevant standards are mature.**

AHIP and our members are firmly committed to providing consumers greater price transparency to aid in their decision-making and empowering them to choose health care services that are both affordable and right for them. Health pinsurance providers offer transparency tools that give consumers estimates of anticipated costs and ways to compare services based on price, quality, and accessibility. **As CMS develops its final rule, we urge consideration of the unintended consequences of the release of granular pricing data on the progress private-sector health insurance providers have already made to provide tools and convey useful information to consumers.**

Moreover, while we all agree consumers should be empowered to shop for health care and make their own decisions, this has not traditionally been the case. Health insurance providers are actively working to increase the use of their consumer tools. Efforts to increase health literacy, share where and how to access information, and encourage incorporating the information into health care choices will benefit everyone. **ONC and CMS should work with stakeholders in a public-private partnership to harness ongoing innovations to ensure consumers have the information they need rather than creating a federal mandate.**

As CMS considers ways to encourage greater price transparency, it is important to recognize meaningful transparency for patients means understanding the expected costs for them individually and should consider not just price but quality and accessibility. Information on the relative cost and quality of a service is most relevant when included as part of shared decision-making between the consumer and the referring physician. We are concerned prices alone for many items and services, without context, could have unintended consequences for consumers. Health care providers are in the best position to provide this context in partnership with consumers and their health insurance

providers, and **we urge CMS and other regulators to seek ways to work with the provider community in engaging in shared decision-making with their patients around costs.** We stress the important difference between the price of a service and the consumer's cost associated with a service. What matters to patients is their out-of-pocket costs based on their specific health insurance, taking into consideration that the patient's financial obligation can vary throughout the year depending on the structure of their plan. We also note that in some circumstances, there may be only one treatment option, while in others, services can be quite 'shoppable.' These shoppable services (e.g., MRIs) are the most relevant to the patient and present an opportunity to test price transparency changes. **Any potential price estimates in future versions of the U.S. Core Data for Interoperability (USCDI) or a future definition of EHI should focus on consumer out-of-pocket costs displayed in a fashion that does not divulge trade secrets, and they should be tested initially with a defined set of services that are effectively shoppable by consumers.**

Requiring public disclosure of pricing data could have potentially 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."[9] 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 are inconsistent with existing Medicare Advantage and Part D non-interference statutory frameworks.[10] Should disclosure of private contract negotiations be required, the cost impacts could be significant, causing serious disruption to our health care system to the detriment of consumers. **CMS should not require the disclosure of negotiated provider rates and ensure any proposal related to pricing information protects market negotiations between health insurance and health care providers.**

There are other ways to provide useful information to consumers without disclosing contracted information or trade secrets. This could include, for example, providing composite value scores comprised of cost, quality and patient experience information, where the negotiated amount cannot be backed into like co-insurance.

CMS should work with ONC to adopt the content standards being develop by the industry through the work of the HL7 DaVinci Project and CARIN Alliance over time. However, CMS should only require the exchange once the relevant FHIR-based standards are established and begin with what is most useful to patients: patient name, diagnoses codes, procedure codes, drug codes, service date(s), provider of service, and out-of-pocket costs. This should not include negotiated rates or any other information that could reveal trade secrets. CMS specifies that the data source should include adjudicated claims that are approved or denied. We are concerned that sharing data, particularly enrollee cost-sharing, on certain types of denied claims will lead to confusion and misinterpretation of claims information by patients or developers. Claims denial information varies. There are many reasons why an issuer may deny a claim that do

[9] 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.**
[10] 42 U.S.C. 1395w-111(i); 42 U.S.C. 1395w–24(a)(6)(b)(iii).

not ultimately result in a denial of coverage. That is, the administrative use of a denial does not necessarily align with a consumer's understanding of denial. For example, some "denials" indicate a service will ultimately be paid. This may include but are not limited to: denial of duplicate claims; claims with missing information that are denied then resubmitted with the correct information; claims denied by a QHP because Medicare is the primary payer and Medicare must submit first; services submitted by a provider that must be submitted by the facility; mutually exclusive procedures. The list of denial reasons that do not indicate a true denial of service—in the manner that a consumer would understand as a denial—is long. **To avoid confusion or misinformation, we recommend health insurance providers only be required to make available data on denied claims in which the service was not ultimately approved, and only once the relevant FHIR-based standards are established.**

It is important to note that the accuracy of the data included in claims is dependent on what health care providers send to health insurance providers. While significant resources go into data integrity efforts, health insurance providers cannot ensure the accuracy of all of the information contained in a claim, particularly that which is not used for payment purposes. **CMS should make it clear that these policies do not mandate that health insurance providers audit and correct all information furnished by healthcare providers beyond what is currently necessary for existing rules, regulations and internal business purposes.**

Timeframes for Data Availability

In general, plans would be required to make these data available no later than one business day after the claim is adjudicated or the encounter data record is received. We agree that claims and other health care data provided through the API with the approval of an enrollee should be accessible in a timely manner. We furthermore understand that the goal is to automate as much of the process as possible, which would easily permit a quick turnaround. However, we contend there are certain circumstances in which a one business-day time frame is neither appropriate nor feasible. Moreover, this proposal does not consider that it may be overall more efficient to have health information exchanges (HIEs) or networks provide the open API for multiple entities than each individually, which would require more time being built in for the transfer. **We urge CMS to work with health insurance providers and other stakeholders to determine appropriate and reasonable timeframes for the various data categories and how these timeframes can be phased in over time instead of finalizing stringent timeframes that are not achievable or advisable for some types of data as outlined below.**

Similar to denials, we are concerned about the timeline applied to claims and data that may be in appeal or otherwise incomplete. CMS indicates that it would apply the one business day timeframe on adjudicated claims including "claims data for payment decisions that may be appealed, were appealed, or are in the process of appeal." We question the value of third-party application use of claims data when an enrollee has filed an appeal and is awaiting a reconsideration decision. The availability of appealed claims data should not be measured from the initial claim or even the appeal, but rather from the final determination of the appeal being entered electronically into the claims payment system.

In terms of encounters where there is no payable claim, CMS should make it clear in the final rule that those health insurance providers who delegate risk to their contracted health care providers and do not obtain encounter data back from the provider would not be required to seek such information or be subject to this requirement. Most capitated provider arrangements do not require the provider to collect or submit to the plan encounter data, which is one of the advantages of such models to providers. Moreover, many capitated providers are small physician practices that do not have the technical or administrative ability to capture and submit this data. The financial and administrative burden that would be imposed on such providers is presently not provided for in the capitation fee arrangements. Consequently, all of those provider contracts would have to be re-negotiated and the cost for the providers' services will necessarily go up, thereby ultimately raising the price individuals pay for care. For those that do obtain claims or encounter data back from those providers, there are existing challenges in the transmission and acceptance of such data and new compliance requirements might have a chilling effect on internal projects to better integrate with providers. As interoperability delivers on its promises, market pressures will drive health insurance providers to deliver functionality that members can use.

While CMS proposes a deadline of one business day after adjudication, CMS also notes it is considering setting a deadline in terms of the number of days from the actual encounter. An encounter-based deadline would put health insurance providers in the position of having to police provider submissions to the plan in order to meet the requirements when the health insurance provider may not even know all of the specific providers within a group of delegated risk providers such (e.g. anesthesiologists, emergency room physicians, behavioral health specialists, and physical therapists). Moreover, rushing the provider submission could decrease encounter data accuracy. Even a deadline of one business day from adjudication, could result in the release of inaccurate or incomplete encounter data. This in turn could confuse enrollees and/or cause harmful unintended consequences if relied upon in making clinical decisions.

Furthermore, a one business-day timeframe is not feasible for services in which plans rely upon third-party subcontractors to adjudicate claims. The migration and quality assessment of data from one system/entity to another could take longer than one business day. In addition, claims may be transmitted in batched transactions where the age of the claims vary. CMS should therefore not impose a one business day limit for data availability for subcontracted services and/or allow separate APIs for these services.

Finally, consistent with our comments above on phasing in the requirements, we recommend that timeframe requirements at the very least should not apply to data for supplemental benefits offered by MA organizations or other issuers. As part of the phase-in process that we are recommending, CMS should begin with medical and pharmacy claims before considering additional types of information (e.g., dental benefits).

In summary, we currently do not support CMS' proposal to impose a one business-day deadline for the availability of claims and encounter data for the reasons outlined above. In phasing in these requirements CMS first should focus on the claims directly adjudicated by plans to hone the technology and allow for a quicker turn-around time in the future and for other data sources. **CMS should revise the requirement to "when available" until it is able to work with the suggested**

industry stakeholder group to determine realistic timeframes for claims adjudicated by the plan, third-party contractors, and delegated risk providers and then propose revised timelines in subsequent proposed rulemaking for public comment. Furthermore, CMS should clarify that health insurance providers can rely on third parties to, such as HIEs, to satisfy the requirement to make such information available through open APIs.

III.C.2 c (3) Clinical Data

When appropriate clinical data is easily shared across stakeholders, patients will be empowered to take better control of their health and make more informed decisions about their health care. To achieve this goal, clinical data should be easy to understand and relevant to the patient's health or treatment. In addition, interoperable data offers providers information to support care planning, treatment, and quality improvement, and provides health insurance providers information to support care coordination and simplify coverage determinations. Clinical data, in addition to claims data, is critical to providing a more complete picture of the health and health care of a patient.

Standard

The proposed required content includes information health insurance providers have available that are in the U.S. Core Data for Interoperability (USCDI) standard (e.g., lab results). Health insurance providers do not commonly collect information in the current USCDI, which is geared toward providers and electronic health records (EHRs), but as health care coordination advances, we can expect to see more coordination between payers and providers' records. In the immediate future, CMS should seek the information from providers to ensure the most up-to-date, comprehensive, and relevant clinical information is shared with consumers. Moreover, we believe that patients would prioritize the clinical information from hospitals and clinicians over that of health insurance providers. As USCDI data elements are standardized in a FHIR-enabled format, comprehensive clinical data may be the best way to achieve the use-cases in the payer-to-payer transactions, reducing unnecessary care, streamlining prior authorizations, and auto-populating risk assessments. **At present, however, the requirement to share comprehensive USCDI through open APIs to third-party apps should apply to providers and their EHR vendors as the originating source and comprehensive view of the patient, not health insurance providers that have fragmented secondary information collected for narrow purposes.**

We understand that the Health Information Technology Advisory Committee (HITAC) chose not to include pricing information in the USCDI at this time, recognizing there is a lack of stakeholder consensus in this area. We do not believe that pricing information, particularly granular level data, belongs in the USCDI—which is a clinical not administrative standard. We directly address the ONC questions about including pricing information in the past, present or future as part of the definition of electronic health information in our comments on that proposed rule. And note, we address pricing information in paid claims above.

API Content

Clinical information is furnished to health insurance providers (sometimes in electronic format) for administrative purposes, quality reporting, risk adjustment and utilization management. While clinical data is essential to get the payer-to-payer transaction to achieve the goal of providing continuity of care when someone changes issuers, this information is not generally helpful or useful at an individual patient level, through the payer-to-consumer transaction. For example, quality measures must be calculated across a population to be valid. In addition, both quality metrics and risk adjustment scores would not be understandable to patients without other population-level metrics that are proprietary to the health insurance providers. Moreover, quality information is generally already available to enrollees in the plans' web-based technologies. If third-party app developers wish to develop their own quality measures (which is inadvisable given the move toward alignment), calculate them, and display them for consumers, it can do so through accessing the basic claims information from health insurance providers and the clinical information for the health care provider APIs. Finally, while health insurance providers may have lab results, for example, as part of a prior authorization request, there is no guarantee that it is the most recent value or represents the complete picture of the patient's health, potentially causing confusion. Thus, we are unclear what information in the possession of health insurance providers and covered under the CMS proposal would be useful to consumers. We believe clinical information from the payer would be valuable in the payer to payer communications for care coordination such as step therapy status as we discuss below. **Sharing clinical information via the open API to third-party apps should not be required of health insurance providers, but rather sought from providers as the source of truth.**

Timeframes for Data Availability

If CMS were to proceed with requiring health insurance providers to share clinical information, a one business-day timeframe is too short. Information obtained from providers is often delivered via phone or fax and may be stored as pdf files rather than integrated into the electronic systems. Thus, while the files may be in a standard format, the files may be in a format that is not compatible with the API. **If CMS requires health insurance providers to make clinical information available, CMS should not mandate a specified timeframe until CMS works with the recommended industry workgroup to determine an appropriate timeframe that allows for standards development, technology deployment, and adequate testing.**

<u>III.C.2.c(2) Provider Directory Data</u>

CMS proposes that MA organizations, Medicaid managed care plans, CHIP managed care entities, and state Medicaid and CHIP agencies that operate FFS systems to make their provider networks available to enrollees and prospective enrollees through API technology. CMS also proposes to except QHPs from the requirement as they are already required to make provider directories public in machine readable files. **We support CMS' proposal to except QHPs and further recommend CMS clarify that a hardship exception application is not necessary for QHPs**
Health insurance providers are committed to providing accurate information in provider directories and work continuously to improve the quality of the directories made available to our members. Health insurance providers are subject to several federal requirements to keep provider directories up

to date. In addition, at least, thirty-nine states also impose state-specific provider directory requirements. For example, QHPs in FFE have been subject to requirements to provide machine readable provider directories since 2016 and have learned many lessons about the operational and technical barriers to enabling the consumer experience envisioned in the proposed rule as it regards provider directories. Experience with QHP machine readable files highlighted two formidable barriers that present major challenges to achieving seamless electronic access to accurate provider network participation status for a specific consumer or patient: (1) Providers do not consistently provide updates and (2) there is no single source-of-truth for provider information that can be leveraged to support tools that rely on machine readable provider directories or apps obtaining provider information through an API. If these barriers detailed below are not addressed, making provider directory information available through APIs as proposed in the rule will not enable successful digital curation and the seamless electronic access CMS seeks to achieve.

Standard

We believe there is a new opportunity to improve the accuracy of provider directories using enabling technology. AHIP members are beginning to test block-chain, for instance, to create a Hyperledger that need be updated by a provider in only two places for the corrections to flow to all additional parties. This technology dramatically decreases the burden on health care providers and increases the accuracy of the information for consumers and health insurance providers. Moreover, there are not yet companion FHIR-based standards. **Thus, CMS should remove the open API requirement for provider directories. Instead**, **CMS should invest in a voluntary multi-payer initiative that seeks to develop standards (content and technical) to support a technology enabled single source of truth for all directories can rely on, test the standards among volunteer stakeholders (CMS, plans, providers, vendors) using open APIs, and then set an appropriate adoption date for the rest of the field.**

CMS proposes to require that the directory data be made available through both the patient-mediated process as well as more widely for prospective enrollees. CMS notes that health insurance provider can make this available through a single API or separately through multiple APIs. Given that one process requires patient authentication and the other does not, health insurance providers may want flexibility on how to make the information available. **We support CMS' proposal to allow this widely-available information to flow through a different API than the patient-mediated information.**

API Content

Open APIs can connect health insurance providers, vendors, healthcare providers, and third-party apps to seamlessly share information. However, the underlying provider directory data is not standardized nationally. For example, the Symphony Provider Directory in California includes additional detail not included in other efforts to account for physicians practicing across different medical groups and/or integrated practice associations in those markets. CMS proposes that Medicare plans make available provider information including name, address, phone number and specialty. For Medicaid managed care plans CMS proposes plans make all the elements including: name, address, phone number, website, specialty, whether the provider accepts new enrollees, cultural and linguistic

capabilities, and whether the office has accommodations for people with disabilities. Existing requirements for QHPs include these provider elements: network, network tier, national provider identifier (NP)I type, in-network plans, name, address, phone, accepting new patients. In order to provide consumers with clear actionable information about the providers in their network, the disparate content standards need to be reconciled at the national level. Until standards are mature, inconsistency in what data elements are required between programs, provider data released today via API would be very difficult for third-party app developers to make sense of and would likely lead to errors in displaying the network status of providers.

In addition to establishing mature standards, steps must be taken to increase the accuracy of information and frequency of updates furnished by providers to ensure that third-party apps can leverage and consumers can rely on the directories. Health insurance providers routinely encourage providers to update their information and provide a variety of methods for them to communicate these updates (e.g. through dedicated provider service telephone lines, online updating forms, contract provisions, etc.). However, health insurance providers' efforts to ensure that provider directories are up-to-date and accurate can be challenging because providers often do not notify the issuer of changes or the subjective nature of a provider's capacity. Changes that health insurance providers rely on health care providers to report include but are not limited to: they stopped or started accepting new patients; they moved their office or added an additional practice location; their phone number changed; they changed specialty or they are no longer practicing in the area covered by the plan.

Today, there is no single source of truth for information on unique providers and the corresponding data elements required for a provider directory. The FFE leveraged the National Plan and Provider Enumeration System (NPPES) to normalize the machine-readable provider directory data provided by QHPs in the FFE. Through this process, several issues with NPPES were identified that interfere with the goal of making it easier for consumers to find a specific doctor and the accuracy of information provided. For example, one facility may have multiple national provider identifiers (NPIs), with some health insurance providers using one NPI and other carriers using others.
In 2016 AHIP launched a pilot program to test different approaches to reducing the administrative burden on providers to update provider directories and increase the accuracy of the information in the directories. Two approaches were identified and over 150,000 providers were contacted to use one of the new approaches to provide updates for provider directories to the health insurance providers networks in which they participated. In both pilots, only 1 in 5 contacted providers furnished complete responses to requests to update their information.

We believe CMS should pursue a pilot project like the current CMS Document Requirements Look-up Service pilot and leverage standardized exchanges of information across disparate parts of the health care ecosystem to address issues with the usability of provider data and at the same time reduce burden on stakeholders. The pilot should: (1) identify which data elements are critical to improving consumer access to provider directory information and define standards for those data elements; (2) establish technology standards for the interoperable exchange of the information and (3) drive the definition of processes that reduce the administrative costs of maintaining provider directories on both providers and health insurance providers. We recognize that CMS may want to explore whether this goal can be achieved by improving NPPES and its new API functionality, but

we suggest CMS also explore whether another solution might be more efficient and effective. For example, a block-chain solution in this area would allow for the secure and seamless exchange of information across stakeholders with clear provenance. **CMS should establish a national, voluntary, multi-stakeholder, public-private partnership that employs a distributed data model by which various vendors, provider groups and health plans can share updates to provider data.**

Timeframes for Data Availability

CMS proposes that updates be made available within 30-days of the change being made. Once standards are in place, the pilot project has been completed and CMS' related report on key findings and recommendations has been released, CMS should revisit the issue of timing. **CMS should wait to establish a required timeframe for provider directory changes until the content and exchange standards are established and a technological solution is developed. At minimum, CMS should allow batch uploads rather than a rolling 30-days from each change.**

III.C.2.c.(4) Drug Benefit Data, Including Pharmacy Directory, and Formulary Data

CMS seeks to improve the accuracy and electronic availability of pharmacy directory and drug benefit information. Thus, it would require MA organizations, state Medicaid and CHIP FFS programs, Medicaid managed care plans, and CHIP managed care entities to make their provider networks available to enrollees and prospective enrollees through API technology. These plans must also make available any drug benefit data, pharmacy directory (except QHP), formulary, or preferred drug list formulary information (for MA Prescription Drug (MA-PD) plans) or information about covered outpatient drugs and preferred drug lists (for state Medicaid and CHIP agencies, Medicaid managed care plans, and CHIP managed care entities).

Standard

QHPs in FFE have been subject to requirements to provide machine readable provider directories and drug formularies since 2016. **We support CMS' proposal not to impose API requirements on QHPs in the FFEs and instead maintain the existing public machine-readable files requirement.**

Timeframes for Data Availability

As noted above, more work needs to be accomplished to solve the operational and technical barriers to enabling the consumer experience envisioned in the proposed rule as it regards provider directories. CMS indicates in the preamble on page 7634 that for MA-PD plans, it is "not proposing a specific timeframe for pharmacy directory or formulary information to be available (or updated) through the API." **We support CMS' proposal related to MA-PD plans and further recommend that CMS refrain from imposing any timeframe requirements across all programs including Medicaid at this time.**

III.C.2.i. Exceptions or Provisions Specific to Certain Programs or Sub-Programs

Excluded Programs or Sub-Programs

Throughout the proposed rule, CMS proposes requirements for MA programs, Medicaid and CHIP FFS programs, Medicaid managed care plans, CHIP managed care entities, and QHP issuers in FFEs. CMS specifically indicates that standalone dental plans (SADPs) in FFEs are excluded from the proposed requirements. However, there are other health plan types or sub-programs for which it is not clear whether these requirements would apply. We believe it is not CMS' intention to include other specialty plans or sub-programs and recommend the final rule explicitly state the following plan types are not required to meet the open API requirements: Medicare-Medicaid Plans (MMPs), Medicaid managed long-term services and supports (MLTSS), and dental plans.

Medicare Advantage and Medicaid

CMS indicates that this proposed rule is applicable to MA Health Maintenance Organization (HMO), point of service (POS), and preferred provider organizations (PPO) plans but does not cover Cost Plans, Prescription Drug Plans, or Program for the All-inclusive Care for the Elderly (PACE) organizations. **We support these proposed exceptions and recommend that CMS also explicitly exclude from the requirements of the rule MMPs, which continue to operate under demonstration authority.**

While Fully-Integrated- Special Needs Plans (FIDE-SNPs) provide Medicare-covered services, many of the Medicaid-covered social and support services they and MLTSS plans arrange for occur in settings well outside of the scope of standard code sets and EHRs. And many LTSS providers that contract with FIDE-SNPs and MLTSS plans – wheelchair ramp installers, personal care attendants, Meals on Wheels programs – have little or no experience with the electronic records that would drive the interoperability sought by CMS in this proposed rule. **CMS also should consider excepting or modifying requirements of the rule as they apply to FIDE-SNPs and MLTSS plans.**

Dental Coverage

In proposing new certification requirements related to exchange of health data and plan information at 45 CFR 156.221(a), CMS specifically proposes to exclude standalone dental plans (SAPDs) from the open API requirements. We agree that implementation of API technology would be overly burdensome and costly for SADP issuers and could inhibit participation in FFEs. It is not clear how such information would be included, as USCDI does not currently include dental information. More broadly, we agree with CMS that the that utility for API access to information via API is less applicable to dental coverage. **Thus, we support excluding SADPs in FFEs from the open API requirements and the exception certification process. We further recommend CMS clarify in the final rule that dental coverage under a QHP (i.e., embedded in the medical benefit), MA, and Medicaid managed care coverage are also excluded.**

Exceptions Process for QHPs in FFEs

CMS proposes an exception process for QHPs in FFEs whereby QHPs may meet the requirements for QHP certification without providing patient access to data through an open API. To apply for exception a QHP issuer must submit a narrative justification providing reasons why the issuer cannot meet the open API requirements, the impact of non-compliance on enrollees, the current means of providing health information to consumers, and proposed timeline to comply with the API requirement.

An exception process should not be a substitute for a reasonable implementation timeframe. We recommend CMS not adopt an accelerated implementation timeframe, as discussed below, with a broad exception process. We believe all stakeholders should work toward the same goal under a reasonable implementation timeframe, rather than an impractical implementation date with all issuers applying for an exception in early years. However, even with a reasonable implementation timeline, not all issuers will be able to comply with the API requirement at the same time. In such cases, an issuer should not be denied QHP certification if it is working in good faith to implement API technology. Without an exception process in place for issuers still working to come into compliance, consumers may face fewer options for coverage through the exchanges or bare counties, with no exchange coverage available. **We support the proposed exception for certain QHP issuers in the FFEs to ensure consumers continue to have access to coverage and financial assistance through FFEs while issuers work to implement API technology.**

CMS specifically proposes limiting the exception to certain scenarios, including small issuers, issuers who are only in the individual or small group market, financially vulnerable issuers, or new entrants to the market for whom deploying API technology would be a barrier to market participation, and not certifying them would result in few or no plan options in certain areas. We support these exception categories but recommend CMS further expand them. Specifically, the last exception should be expanded to both new and current QHP issuers for whom compliance would pose a significant barrier to offering QHP coverage to consumers. **We support the proposed scenarios in which a QHP issuer may be eligible for an exception. We further recommend current QHP issuers who are not yet able to implement API technology also be eligible for exceptions. No issuers currently offering coverage in the FFEs should be denied certification because they are not yet able to make patient data available via open APIs.**

CMS should provide additional information on the exception process through sub-regulatory guidance. This should include additional details on what information issuers should include in the narrative justification, criteria CMS will consider in reviewing exception apps, and other guidelines for the timeline and approval process. Any issuer who requests an exception must demonstrate clearly, though the exception process, how they are working towards compliance. CMS should also specify how justifications will be submitted (e.g., directly to CMS or incorporated into HIOS and SERFF systems for plan filing). **We recommend guidance be included in the annual Letter to Issuers in the FFEs to provide issuers time to understand the requirements and process to apply for an exception.**

Extend Exceptions Process to Other Plans

CMS proposes to provide an exceptions request process that would be limited to issuers participating in the FFEs. However, we believe any plan type could face challenges or hardships that would necessitate an exception. For example, small issuers or new entrants participating in any of the impacted programs could face challenges that warrant an exception to the API requirements. **We believe the exceptions process should also be extended to plans that participate under the MA, Medicaid, and CHIP programs.**

III.C.2.j. Applicability and Timing of the Open API

CMS proposes the following effective dates for implementation of the proposed API requirements and requests comments on the timing, including feedback on the amount of time health insurance providers anticipate it would take to come into compliance with CMS's proposed API requirements:

- Medicare Advantage organizations and Qualified Health Plans issuers in Federally Facilitated Exchanges (FFEs) – the effective date would be January 1, 2020.
- Medicaid fee-for-service (FFS), Medicaid managed care organizations and CHIP managed care entities – the effective date would be July 1, 2020.

We share CMS' vision of making health information more accessible by consumers. Today, health insurance providers make available patients' health information by electronic means, and some are already undertaking efforts to make this data interoperable. but much work remains to make health care data truly interoperable. We agree that CMS' proposed API solution would help to address many of the gaps in today's health care system, and the largest gains from interoperability are only possible when underpinned by national standards. However, it is worth taking the time to implement this vision effectively. A rushed implementation could lead to a lack of trust in the effort and leave consumer health information exposed to security risks. **The proposed timeframe for implementation by 2020 is unrealistic and could lead to negative unintended consequences for patients.**

We strongly urge CMS to finalize a staggered compliance deadline, consistent with previous adoption of landmark health IT regulations. This would provide additional time for standards to mature, industry to address outstanding questions related to the protection of patient data accessed by third-party app developers, and for health insurance providers to develop, test, and implement API technology. **The implementation timeline for the open-API should be phased-in, tied to the development of relevant standards, with full compliance starting no earlier than 2022.** A phased implementation will provide time for CMS and stakeholders to resolve the many known—and yet unknown—challenges to implementing open APIs.

To achieve compliance by 2022, a phased implementation approach should include each of the following milestones:

- Finalization of the proposed rule and promulgation of sub-regulatory guidance;

- Maturity of standards, vocabularies and code sets, and other technical requirements;
- Development of privacy and security protections for patient data accessed through third-party apps not subject to HIPAA including vendor vetting;
- Development, testing, and implementation of the technology, in addition to resources and customer support, to comply with open API requirements;
- Development and testing of model language on disclosure of patient information to third-party app developers for use by health insurance providers, health care providers and apps, ahead of implementation and on an ongoing basis.

As discussed elsewhere in our comments, maturity of standards and ensuring privacy and security protections for patient data are of paramount importance when considering an appropriate implementation timeline. However, CMS must also consider operations and compliance aspects of implementing open APIs as well as existing bid cycles and certification timelines for MA plans, Medicaid managed care plans, and QHPs in the FFEs.

Health insurance providers cannot fully assess the impact of the proposed rules or begin efforts to comply with the open API requirements until a final rule is published. Until that time, there is significant uncertainty in the scope of the requirements, timing, etc. Once the final rule is published, health insurance providers will still need significant sub-regulatory guidance in order to establish a strategic development plan, including budgeting for significant systems changes, IT project planning, and significant systems development to build, test, and deploy API technology. Most issuers anticipate a project of this scale would take two to three years after publication of final rulemaking to make the systems and operations changes needed to come into compliance.

A 2020 compliance deadline is further infeasible due to the timing of bid cycles and certification timelines. Bid cycles and certification timelines are well-established through federal and state statute and regulation. Issuers are currently working to meet state filing deadlines and federal bid and certification deadlines for the 2020 plan year. MA plan sponsors must submit 2020 bids by June 3, 2019 at the latest. QHP issuers in the FFE must submit the QHP application by June 19, 2019. This rule will not be finalized by those deadlines, making it impossible for issuers to be ready and demonstrate compliance with the proposed API requirements as a condition of participation/approval or incorporate cost estimates into bids. CMS acknowledged this it its notice delaying the comment deadline stating that the implementation date would be altered accordingly. We anticipate that the final rules, from both CMS and ONC, will not be released until the fourth quarter of this calendar year, which renders a 2020 start date infeasible.

There are, however, some health insurance providers that were already actively participating in the standards development process and building such technology that could be ready earlier. **During 2020 and 2021, CMS should consider a testing period with volunteer health insurance providers to learn from early adopters and allow those plans to count the open API development costs as QIA under the MLR.**

Below, we provide additional program-specific considerations related to the proposed effective date.

Medicare Advantage

We believe the 2020 effective date for MA plans is infeasible for several reasons. First, CMS' proposed effective date fails to consider the MA bid deadline. CMS published its guidance on methodology changes and other matters of key importance for MA bids on April 1, 2019. Plan sponsors use this CMS guidance to finalize and submit 2020 bids by the statutory June 3, 2019 bid submission deadline. However, since comments on the proposed rule are not due to CMS until June 3, 2019, it is not possible for CMS to comply with its obligation to give MA plans clear guidance on the regulatory environment and obligations to assume in their bids. An actuarially sound bid requires plans to be able to project relevant costs including those associated with implementing the proposed API requirements. The Final Notice and Call Letter failed to include instructions regarding how plans should estimate such costs.

Second, MA plans, like other plans, need sufficient lead time to take operational, contractual, and other necessary steps to comply with the final API requirements. For example, many MA plans work with vendors to implement major changes to their health IT systems, and these changes will need to be effectuated through contracts that require time to negotiate and execute. And any new approach, particularly one requiring the development and testing of costly new systems and capabilities and a range of other operational actions such as this Proposed Rule, must have an appropriate transition period. According to the American Academy of Actuaries, significant changes to regulations should be proposed at least two years prior to their effective date to enable health insurance providers and their actuaries to "make the necessary operational and bidding changes to accommodate them."[11] Third, there is a need to develop, test, adopt and implement the various standards that the industry will need to use in order to achieve the health insurance provider information exchange transactions defined in the regulation. Naming of such standards should be done by ONC, and adoption and use should follow the same timeline being considered by ONC in its regulations of 24 months after the publication of the final rule.

Medicaid FFS, Medicaid MCOs, and CHIP managed care entities

The 2020 effective date is also not feasible for the Medicaid program. Considering the timing of the proposed rule and its rapid implementation timeline, we are concerned that states, their Medicaid agencies and Medicaid health plans have not had an adequate opportunity to plan and budget for the work needed to implement the requirements envisioned in the proposed rule. States legislatures and Medicaid agencies set their budgets and Medicaid payment rates in advance, with budgeting and contract years often varying from the federal fiscal year cycle. In addition, many state legislatures are in session for only part of the year including some that only meet biennially and 32 states will have concluded their 2019 legislative sessions by June 1, 2019. For most states, because the regulation has not been finalized legislators have not allocated sufficient infrastructure funding to the Medicaid agencies to support the effective implementation of all the requirements in the proposed rule. Beyond the appropriation of funds necessary to support the infrastructure build, states need to adhere to competitive procurement processes to contract for IT system changes, and those processes often take many months.

[11] https://www.actuary.org/sites/default/files/2019-04/Rx_Rebate_Timeline_04032019.pdf

In the absence of concrete standards, final regulations, and operational guidance for the sweeping changes contemplated in the proposed rule, there is not enough time to contract with IT vendors and perform the work in time to meet the deadlines. Furthermore, it is an open question whether there are enough IT vendors with the correct subject matter expertise available to make all the system modifications needed to develop, test and implement the requirements of the proposed rule in each of the 56 Medicaid jurisdictions. Given the technology and security implications of the rule for the protected health information of American consumers, IT system changes should be made only by qualified and vetted IT resources. Given these limitations and the scope of the proposals, the IT services contracting, development, testing, and implementation pipeline would take years.

With respect to Medicaid programs, given the lack of final standards and the magnitude of the requirements, we recommend that CMS allow at least five years for implementation. Further we recommend that CMS work with State Medicaid leaders to identify an appropriate glidepath and milestones. It should be noted that the implementation of the provisions of the rule will divert limited state and IT vendor resources away from another CMS priority: completing the implementation of the Transformed Medicaid Statistical Information System (T-MSIS). Although states are now submitting Medicaid data directly to CMS, we understand there are still challenges with the completeness and timeliness of the data. We strongly recommend that states complete the T-MSIS implementation while allowing for the completion of the final standards necessary for the implementation of the proposed rule and, when T-MSIS is fully implemented, move forward with implementation of the provisions of the then final rule.

With regard to Medicaid managed care organizations (MCOs), we note that 38 states, Puerto Rico, and the District of Columbia use managed care arrangements to manage care and services for more than 75 percent of Medicaid enrollees nationwide as of 2018.[12] However, many states that use Medicaid managed care exclude certain populations from those Medicaid managed care programs. **In order to allow for effective implementation across all parts of a given state's Medicaid program, we recommend that the implementation timeline for Medicaid managed care plans align with that of the state Medicaid agencies.**

We have significant concerns regarding the costs of implementing the sweeping new capabilities contemplated in the proposal and how these new capabilities will be paid for in the Medicaid program. The CMS proposal notes that

> ...state Medicaid agencies may be allowed to allocate the costs of state information retrieval systems between the costs attributable to design, development, installation, or enhancement of the system—at a 90 percent federal match—and for ongoing operations of the system—at a 75 percent federal match. For Medicaid Managed Care entities, we assume an MCO, PIHP, and PAHP cost for implementing the open API provisions would be built into the capitation rates and matched at the State's medical assistance match rate.

[12] *Medicaid Atlas* produced for AHIP by Health Management Associates, May 2019.

CMS should make an affirmative commitment that states will be allowed to receive appropriate enhanced federal matching funding for costs of modifications to their information retrieval systems and that the states should include such costs in the MCO's rates.
In addition, we are concerned that reimbursing states for modification of their IT systems at an enhanced match rate while reimbursing MCOs for their system modifications at the state's standard match rate creates an unlevel playing field for Medicaid MCOs and a disparity of funding. In states that make extensive use of managed care, the bulk of system modifications needed to carry out and maintain the proposed interoperability capabilities for Medicaid enrollees will be borne by Medicaid MCOs. In this respect, the proposal asks states with strong managed care programs to pay a greater share of implementation costs than states that operate unmanaged fee-for-service programs. **Therefore, we ask that CMS revise its proposal to reflect that all costs attributable to design, development, installation, enhancement or ongoing operation of both state and Medicaid MCO systems will receive the appropriate enhanced federal match.**

Additionally, the proposal states that CMS *assumes* MCO, PIHP, and PAHP costs for implementing the open API provisions would be built into the capitation rates. **We request that CMS take a more rigorous approach to this issue and update its methodology for review of state MCO capitation rates to ensure that proposed rates include reasonable allowances for costs of IT systems work performed by the state's Medicaid MCOs in furtherance of this proposed regulation.** We believe that this additional step is necessary to ensure the integrity of capitation rates consistent with the actuarial soundness provisions at 42 CFR 438.4.

Finally, we note that the extraordinary IT system expenditures resulting from this proposal would significantly increase administrative costs. Medicaid MCOs are required to maintain a minimum medical loss ratio of no less than 85 percent (42 CFR 438.8(c)). **We urge CMS to specify in the final regulation that costs associated with development, implementation, and ongoing support of the capabilities and requirements described in the proposal will be recognized as quality improvement expenditures for purpose of the MLR calculations and reporting, consistent with regulations at 42 CFR 438.8(e)(3).**

QHPs in FFEs

CMS proposes to require compliance with open API technology requirements by the 2020 plan year for QHP issuers offering coverage through FFEs. QHP issuers are currently finalizing and preparing to submit their product offerings and rates to state and federal regulators for approval for the 2020 plan year. QHP issuers in the FFEs must submit the initial QHP application to CMS by June 19, 2019 and rates by July 24, 2019.[13] However, issuers are also required to submit products and rates to state regulators for review. While state deadlines vary, states require form filings—which include information about products, including benefits and service areas—as early April and rate filings as early as May 1.

[13] https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Final-Key-Dates-Table-for-CY2019.pdf

To develop appropriate product offerings and rates, issuers need appropriate lead time to understand the impact of major policy changes in order to make decisions about market participation, product offerings, and rates. Further, the certification and exception criteria must be clearly defined in advance, ideally alongside other certification guidance and requirements published in the annual Letter to Issuers in the FFEs. Without final rulemaking or an understanding of the certification criteria or exceptions process, QHP issuers cannot make decisions about market participation, product offerings, or rates for the 2020 plan year. **If CMS finalizes the effective date for the 2020 plan year, QHP issuers would not be able to meet certification criteria to offer coverage through the FFE and consumers would be faced with few or no coverage options in the 35 FFE states. Therefore, we urge CMS to delay the implementation of the proposed rule to align a future QHP filing timeline.**

TRANSPARENCY OF OPEN API

III.C.2.d. Documentation Requirements for APIs

CMS proposes to adopt by reference standards ONC names in its companion Proposed Rule. However, CMS also seeks comment on whether it should adopt new and future standards separately from those adopted by ONC. We are concerned that this approach would lead to two sources of standards for the same information exchange transactions and processes, increasing the possibility of having multiple sets of mandated yet conflicting standards for the same transactions. If the adopted standards were to diverge, the burden on subject organizations would be very significant because different regulatory requirements would complicate the maintenance of standards and systems.

We recommend CMS adopt by reference ONC standards for use in APIs. FHIR standards for app-based exchanges, and the ONC-named USCDI standards (to the extent that they apply to health insurance providers) to align technical requirements across federal programs. Standards (e.g., HL7 FHIR Release 4) and their implementation timelines should be aligned in the CMS and ONC Final Rules. Moreover, the implementation specifications for various uses of these standards should be addressed through sub-regulatory guidance, not by rulemaking. For example, data element specifications to support quality reporting may vary from year to year, so the FHIR profiles containing implementation specifications should be published using a sub-regulatory mechanism that is more flexible than notice-and-comment rulemaking. However, our recommendations are contingent on ONC making every effort to solicit and incorporate stakeholder feedback as part of the process.

CMS notes that transparency about API technology is needed to ensure that any interested third-party app developer can easily obtain the information needed to develop apps that are technically compatible with an API. Health insurance providers must make information publicly available to vendors in order to successfully interact with the API such as any requirements the organization may have for verification of developers' identity and their apps' authenticity, and what the privacy and security protection policies are etc. We caution CMS to avoid using this mechanism as a way for health insurance providers and third-party apps to make up for the shortcomings of existing standards through the promulgation of excessive individual plan API documentation.

CMS also notes on page 7634 of the preamble that ‘‘publicly accessible’’ means “without any preconditions or additional steps beyond downloading and using a third-party application to access data through the API.” CMS goes on to provide collecting a fee for access to the documentation as an example of a precluded ‘‘additional step.’’ If health insurance provider are required to expend funds to build this new technology and maintain it, the costs will be borne by all consumers, not just those who use the apps, through premiums. The business model for these apps hinges on the ability to sell the consumer data to other interested parties for secondary uses. We believe that health insurance providers should be able to charge third-party app developers a “subscription fee” to cover the cost of maintaining the open API. **If developers are monetizing consumer data, they should have to build data acquisition costs into their model to defray the cost of open APIs to the consumer. Otherwise, CMS should allow health insurance providers to include such expenses as a part of “quality improving activity” for the purpose of calculating the plan’s medical loss ratio.**

III.C.2.e. Routine Testing and Monitoring of Open APIs

An API also must be routinely tested and monitored to ensure it is functioning properly, including assessments to verify that the API is fully and successfully implementing privacy and security features required by law. **CMS should define what “routine” means, how they will be monitored, (especially as new threats develop), how testing might work without making the tester a business entity under HIPAA, and how CMS might evaluate the proper function of the API when payers will not be able to see what the function of the apps using the API actually are.** Having regular workgroups with representatives from CMS, health insurance providers, and developers might provide a forum where stakeholders can better understand the other parties’ positions, problems, and goals. Phasing-in requirements, starting with use-cases for the data that are clearly defined and testable will allow the industry to better understand when standards have matured to the point where they can “function properly”.

PRIVACY AND SECURITY

III.C.2.f. Compliance with Existing Privacy and Security Requirements

CMS requests “public comment on whether existing privacy and security standards, including but not limited to those in 45 CFR Part 164, are sufficient with respect to these proposals, or whether additional privacy and security standards should be required by CMS as part of this proposal." Duplicate requirements and conflicting interpretations by various agencies have proved inefficient and difficult to understand/implement even without this additional complexity woven in. The interaction with state laws further complicates understanding and applying the rules appropriately and consistently. **We have, and continue, to support OCR as the primary agency for issuing and interpreting privacy requirements. We encourage OCR to provide additional guidance and further clarification on the application of privacy and security requirements in this context.**

<u>Security</u>

CMS proposes that MA organizations, state Medicaid and CHIP FFS programs, Medicaid managed care plans, CHIP managed care entitys, or QHP issuers in an FFE may deny access to the API if

connecting to that third-party app presents an unacceptable level of risk to the security of PHI on the health insurance providers' systems. This determination would need to be based on objective, verifiable criteria that are applied fairly and consistently across all apps. CMS also notes that automated monitoring and risk mitigation tools can be used as part of such determinations. **We agree that health insurance providers should have the ability to minimize entry points that would make the security enterprise vulnerable to threats and integrate automated processes into security determinations. Additionally, we request additional allowances be considered through sub-regulatory guidance, in consultation with stakeholders, as they arise throughout implementation.**

Individual Authorization

The preamble explains that

> to the extent a HIPAA covered entity uses a third-party apps to offer patients access to their records, another HIPAA covered entity may be able to obtain an individual's health information from the app for treatment, payment, or certain health care operations, if it could do so in accordance with HIPAA without need of an individual's authorization. (See 45 CFR 164.506.) Under other laws, providers may need to obtain specific individual consent to obtain health information related to care provided by a behavioral health provider, treatment received at a substance use disorder treatment facility, certain 42 CFR Part 2-covered diagnoses or other claims-related information, or labs that suggest a Part 2 diagnosis. We [CMS] do not intend to expand any scope of authority to access patient data nor to contravene existing requirements related to disclosure of PHI under the HIPAA Rules and other legal standards, but instead specify a new and additional mechanism by which to share health information as directed by the individual, through the use of API technology in compliance with all existing federal, state, local, and tribal privacy and security laws.

We concur with CMS that the proposed rule simply provides a new path to satisfy an existing requirement.

Utilizing Apps for TPO

We appreciate that CMS clarifies that this is a new path and does not disturb the existing path available to covered entities. The focus on this path should be the sharing of data from either a payer or a provider to a third-party app at the request of a consumer. Interoperability between covered entities should not be dictated here. In fact, we urge CMS to refrain from suggesting that moving PHI from one covered-entity (e.g. plan) through a non-covered-entity (e.g. app) to another covered entity (e.g. provider) is an appropriate path as the intermediate step removes the important protections of HIPAA in the interim. There are other more efficient, effective, and secure routes to accomplish the same interoperability while maintaining HIPAA privacy protections for consumers. For example, many health insurance providers are sharing data with clinical providers as part of HIEs. Once the Trusted Exchange Framework and Common Agreement (TEFCA) proposal is finalized, we

anticipate even greater connections through the "network of network" that TEFCA envisions. **CMS should discourage use of third-party apps for HIPAA covered entities to conduct treatment, payment or operations and should instead focus on the utilization of Trusted Exchange Networks for this purpose.**

Consent and Data Segmentation

As CMS notes, the patient-mediated process for both the payer-to-payer and payer-to-member transactions requires an explicit authorization by the consumer to transfer the information to the app. Assuming the consumer has credentials for the payer portal, then the authentication of the consumer should be seamless. It adds another layer of complexity, however, if the health insurance providers are then expected to determine if that person has a right to consent to the sharing of the data or to provide data segmentation options for sensitive diagnoses due to an overly-broad interpretation of 42 CFR Part 2 or state laws. For example, many states have laws regarding the appropriate age where minors can consent to direct their treatment and thus health insurance providers would need to put in place consideration reflecting the provisions of those laws (e.g., parents cannot have access to claims information). In addition, a state law could prohibit or complicate implementation of these requirements in any form. Clarifying the complex and changing web of state and federal laws will not be imminently accomplished and would not prevent disruption from new legislation. **We believe the onus should be on the app to verify the patient's ability to provide consent before connecting to health insurance providers' authentication process, and health insurance providers should not be held accountable if the apps fail to obtain the proper consent. We also believe that consent to use the API process should be "all-or-nothing" and health insurance providers' current HIPAA compliance processes can be used if state laws, consent issues, or other consumer concerns render the API path inappropriate.**

Furthermore, getting legal and operational designations to mesh to the degree of precision necessary to enable patients to choose which segments of data to share will be contentious, laborious, and run counter to member expectations. Doing so is not possible without making changes to the structure of electronic records and does not exist today. For example, 42 CFR Part 2 attaches to records based on the provider, but state laws may require health insurance providers to filter substance use conditions at the diagnostic level, regardless of the source of the diagnosis, leading to missing information which could potentially aid in treatment decisions and care management. In addition, there is no standardized delineation of "mental health diagnoses," which the Mental Health Parity and Addiction Equity Act (MHPAEA) leaves up to state law or to health insurance providers. Mapping such a distinction on to diagnostic or service codes would require a clinical standards development process, would probably fail to align with certain state laws and would create needless conflict across professional organizations. Inevitably, the distinction drawn whether for mental health or other conditions and services, will not line up with the specific expectation of the consumer. If consumers are concerned that some of their PHI is too sensitive to share with their new payer or too sensitive for their payer to share with them via an app, they can rely on existing HIPAA-compliant mechanisms, rather than the API process. Finally, this kind of segmentation by diagnosis does not exist for EMRs and because FHIR is expected to work with EMRs, a system based on FHIR may share this inability to share a limited set of diagnoses or providers. Warping the API process to accommodate state laws (including ones that might be passed in the future) is not possible. Moreover, in the payer-to-payer

communication, filtering sensitive diagnoses and passing a health insurance provider an incomplete version of the health record could undermine care management and clinical determinations. **Consumers should have the choice to share all or none of their data via the API pathway. If consumers have concerns about specific information, they should be directed to the existing path to obtain information via other means (e.g. CD-ROM) that the patient can segment based on their preferences.**

As we noted earlier, we continue to be concerned about the secondary uses of data permitted under this proposal. We believe that health insurance providers should be allowed some latitude within their agreements with third-party app developers to ensure adequate consent is obtained and that the uses of the data are transparent. **Health insurance providers should be able to require the app to seek consent for each secondary use, to generate an accounting of where the data was shared similar to the HIPAA requirements, or join a Trusted Exchange Network.**

Lastly, we are concerned that the CMS rule suggests that once the authentication occurs that the tokens are open in perpetuity. Consumers may not understand this open-ended access and are unlikely to think about how to revoke access to the data when they delete an app. **CMS should implement a 90-day time frame for the authentication token to remain open comparable to ONC.**

Third-Party Applications Vetting Process

The proposed rule currently contains no certification process for third-party apps. Given the access to personal health information these apps are expected to have and the potential privacy risks they pose, **we recommend that a process be established by the Federal Trade Commission (FTC) in collaboration with the Department to vet apps for the adequacy of the consumer disclosures, the privacy and security of the information once it is no longer governed by the HIPAA and secondary uses are permitted, and clinical soundness (for those apps that offer medical advice).** The vetting process should be at the application level, not just at the application developer level, and the results of such vetting process should be made public in the form of an application "safe list." Additionally, health insurance providers should be able to refuse to connect to non-vetted apps. While CMS and others draw the parallel to use of third-party apps to conduct personal banking, the implications and consequences of a potentially widespread availability of personal health information are arguably far greater. In addition to the current consumer complaints process and to enhance oversight, we further recommend the establishment of a formal process for health insurance providers and health care providers to submit complaints to the FTC about apps that are suspected of misleading consumers, misusing personal health information or otherwise failing to meet basic standards for privacy and security of personal health information. **After evaluation of complaints, the FTC should publicly post a list of apps that do not meet basic standards to avoid continued provision of data to these developers without true understanding by the consumers of the heightened risk.**

III.C.2.g. Issues Related to Denial or Discontinuation of Access to the API

The ONC proposed rule identifies reasonable and necessary activities that do not constitute information blocking. We agree that there are certain instances where an actor might reasonably need to restrict electronic access to data. As stated in our comments on the ONC proposed rule, health insurance providers do not fall within the definition of actors that would be subject to the information blocking provision, as health insurance providers are neither health IT developers, health care providers, health information networks, or HIEs. However, we feel that there are reasonable and necessary circumstances in which a health insurance provider would need to deny or delay a request by a consumer to share data that are in line with ONC's exceptions to information blocking. For example, ONC proposes that an actor may engage in practices or implement measures that protect the privacy or security of electronic health information. We feel a health insurance provider should also have the ability to restrict access to information transmitted via APIs if the manner in which the information is accessed, exchanged or used is not permitted under the HIPAA Privacy Rule, or if the access, exchange or use would compromise the confidentiality, integrity, and availability of the information. For example, if a developer's app design, intentionally or inadvertently, queries the API so frequently that it negatively impacts the issuer's systems, it could be interpreted as a dedicated denial of service (DDOS) attack, and it would be reasonable to expect the health insurance provider to block that app and limit the frequency any app can connect to the API, regardless of whether there was proof that the app intended to compromise the integrity of the health insurance provider's systems. Or, we may have reason to be concerned a third-party app developer has malicious intentions and, therefore, would want to block the connection until due diligence can be completed or the concerns are address, and perhaps even shared with to law enforcement officials. As another example, a health insurance provider can temporarily make the systems unavailable for maintenance. **We recommend CMS rely on continuing conversations with stakeholders to establish and maintain circumstances in which it may be appropriate for health insurance providers to delay or deny a request by a consumer via a third-party app developer. Additionally, we recommend that CMS develop and regularly update FAQs as we learn more though implementation experience.**

III.C.2.h. Enrollee and Beneficiary Resources Regarding Privacy and Security

CMS stresses the need to for health insurance providers to include and emphasize the importance of understanding the privacy and security practices of any app to its enrollees. This information must be in "non-technical, consumer- friendly language" and include information of how to submit complaints. We remain concerned that consumers may not have a full scope of information necessary to understand these situations and the potential consequences of sharing their health information with certain apps. We stand ready to work with our federal partners to help enrollees become more informed about how to protect their PHI, important things to consider in selecting an app, and where they can lodge a complaint if they believe they have been subjected to unfair or deceptive actions or practices related to a direct-to-consumer application's privacy practices or terms of use.

However, while all stakeholders should play a role in patient education regarding data sharing, including health insurance providers, we believe the Department in collaboration with the FTC

should take the lead in educating patients about the differences between HIPAA and non-HIPAA-covered entities, and how those differences may affect the ways in which their data is used, stored, and shared with others. Given CMS' experience implementing the Medicare Blue Button 2.0 initiative as well as the associated consumer education campaign, CMS could leverage lessons learned and apply them to this broader consumer education effort. This education program should advise consumers on what to consider when selecting apps, how the data sharing rules work, and how to safeguard data privacy and security. We believe that consistent language for use in education campaigns across providers, payers and the federal government will hasten the understanding of the public and smooth the transition to interoperable health care data. The Department and the FTC should develop model consumer notifications and education materials for voluntary use by health insurance and health care providers.

In the development of these materials the Department and the FTC should be aware that trying to address privacy concerns with education will be difficult as it requires countering consumers current understanding that all PHI is protected. **Thus, the Department and the FTC should ensure that third-party app developers are also appropriately informing consumers that HIPAA privacy rules will not apply when they agree to share their data with apps and clearly outline all the ways in which they will use a consumer's data in plain language and to insure they are not mislead. The Department and FTC should develop comparable model plain language consumer notification for app developers.**

V. HEALTH INFORMATION EXCHANGE ACROSS PAYERS

CMS seeks to require health insurance providers to share health information in sequence as enrollees change plans to approximate a longitudinal health record that the patient can access through third-party apps. CMS would require MA organizations, Medicaid managed care plans, CHIP managed care entities, and QHP issuers in the FFEs to support electronic exchange of data, at the patient's request and for up to five years after disenrollment, for transitions of care as patients move between these plan types. **We support appropriate sharing of enrollee information between health insurance providers to promote effective coordination and agree that such efforts should count as a quality improvement activity for purposes of medical loss ratio (MLR) calculations.** CMS proposes to require those data types and elements in the USCDI standard, such as diagnoses, procedures, tests results, and providers notes. As stated earlier, health insurance providers are not the source of truth for the bulk of the USCDI. Moreover, the HITAC is considering adding pricing information to the USCDI, which should under no circumstances be shared across health insurance providers. There are, however, some aspects of both claims and clinical information that would certainly be helpful in terms of care coordination from one payer to the next in order to streamline prior authorization, step therapy, and other utilization review requirements. **CMS should not require health insurance providers to share the entire USCDI, but rather focus on the patient-centric use cases in which health insurance providers are the source of truth based on guidance from the technical expert panel.**

Furthermore, we support that CMS is not dictating the means by which the plans share this information. CMS notes that direct exchange, exchange through an HIE, open APIs or other means

would be acceptable. Given that payers already rely on HIPAA transaction sets to share information electronically, it is not clear that API enabled, FHIR-based standards are the best approach for communication of certain information. We note that the HL7 DaVinci project is developing and testing a new FHIR-based standard for implementing health plan-to-health plan information exchange, consistent with the goal set in the proposed rule of care coordination. **However, CMS should allow the private market to determine the best route to accomplish electronic exchange depending on the use case and only require implementation once the associated standards are mature.**

VI. TRUSTED EXCHANGE NETWORKS

CMS proposes to require MA organizations (including MA-PD plans), Medicaid managed care plans, CHIP managed care entities, and QHP issuers in the FFEs to participate in a Trusted Exchange Network (TEN) beginning January 1, 2020. The TEN must meet the following three criteria:

1. The TEN must be able to exchange PHI, defined in 45 CFR 160.103, in compliance with all applicable state and federal laws across jurisdictions.
2. The TEN must be capable of connecting both inpatient EHRs and ambulatory EHRs.
3. The TEN must support secure messaging or electronic querying by and between patients, providers and payers.

Overall, we support CMS' effort to establish a network-of networks policy framework for trusted exchange of health information and its inclusion as a quality improvement activity for purposes of MLR requirements. We agree that more needs to be done to encourage trusted exchange of health information through interoperable systems to support care coordination, care management, and population health. Over the past several years, AHIP has engaged in discussions with the ONC on a wide range of health information technology issues. Pursuant to the 21st Century Cures Act, the ONC outlined a set of principles for trusted exchange and minimum required terms and conditions for trusted exchange in the in its first and now second Draft TEFCA. **The July 1, 2020 effective date and requirements for payers to successfully participate in a TEN, are not attainable today,** and much work needs to be accomplished such as:

- ONC and the new Recognized Coordinating Entity (RCE) will need to develop and socialize in a transparent manner the Common Agreement, a key component required for the Trusted Exchange Network.
- Today suitable Qualified Health Information Networks (QHINs), do not exist and the ability to exchange information between them in a way that will meet the proposed rules technology requirement, and state regulations is yet to be determined a requirement for a successful TEN.
- We need time to evaluate if QHIN's and Health Information Exchanges and Networks can meet our geographic requirements and determine if they have the technical ability to scale their systems to meet our needs to participate in a TEN.
- We would like to better understand the requirements and available incentives for QHIN's to support its participant's and participant members with regard to the TEN.

- Exchange standards are still immature and not fully tested nor available to support plan to plan data exchange through the TEN.
- As stated earlier, the USCDI today does not meet plan data exchange requirements. Clarification is requested if all users, participants, participant members and QHIN's will be required to share USCDI or only QHIN's or QHIN and their TEN participants.
- We will require additional information on how the RCE will monitor the QHIN's and ensure our member's data is being protected and utilized correctly.

We request ONC and CMS allow insurance and health care providers as well as other industry stakeholders adequate time to evaluate and test the TEFCA with all of its enabling components in a transparent manner before requiring them to participate in a TEN. In addition, we recommend the CMS apply such a requirement on healthcare providers at the same time it does so for health insurance providers.

We would like to reiterate several comments we made in response to the first DRAFT TEFCA that are applicable in this context. We support leveraging existing trust networks operating successfully to further advance interoperability, support care coordination, and improve patient access to their data. Significant progress has been made in recent years resulting in more widespread health information exchange. The experience of current health information exchange networks and existing agreements should serve as the foundation for future developments in HIE. **We encourage CMS to support a flexible approach for payer-to-payer and payer-to-provider interoperability that leverages existing networks.**

We also believe there should be a level playing field for privacy and security requirements among those connected through the trusted exchange networks. Individuals, covered entities, business associates, and noncovered entities may all be connected through health information exchange networks. Yet covered entities and their business associates would be required to follow strict requirements about uses and disclosures of identifiable health information under HIPAA while non-covered entities not subject to HIPAA might only have to comply through a participating agreement. **We recommend that this regulatory gap be closed by requiring that all non-covered entities participating in the TEN comply with the same HIPAA privacy and security requirements that apply to covered entities in order to ensure the privacy and safety of health information.**

Should CMS choose to proceed with its Trusted Exchange Network requirements, we are concerned that the third criterion above is too expansive and does not reflect the functionality commonly available in most HIEs today. Most HIEs do not have the ability to generate a secure message, and most – if not all – HIEs are provider-oriented and do not have interfaces or tools that directly connect with patients. If CMS moves forward with the criteria as proposed, plans will likely have very few TEN options. This not only places an undue compliance burden on payers, but also has the potential to negatively impact the competitiveness of the health information exchange market. **CMS should remove its proposed third criterion for eligible TENs.**

We support CMS' belief that activities related to this proposal qualify as a quality improvement activity (QIA) for purposes of the MLR requirements for QHP issuers in an FFE and similar standards for treatment of quality improvement standards applicable to Medicaid managed care

plans, CHIP managed care entities, and MA plans. This helps ease the administrative burden and address the uncertainty that the MLR rules would create if each insurer had to independently prove the value of interoperability. **We urge CMS to retain this qualification as a Quality Improving Activity for purposes of MLR requirements in the final rule as it will create an incentive for capable health insurance providers to be thought leaders and innovators in advance of national implementation.**

Lastly, given that the TEFCA framework may not be finalized by the publication of this rule, health insurance providers will not know what Qualified Health Information Networks (QHINs) that are going to be available and will not have ample time to assess and join within the currently proposed implementation timeframe of 2020. **As such, we recommend that there be an exception process to the requirement to join a TEN that meets the specified criteria if the sufficiency of existing options is poor.**

VII. INCREASING THE FREQUENCY OF FEDERAL-STATE DATA EXCHANGES

Interoperability of state and CMS eligibility systems is a critical part of modernizing the programs and improving beneficiary and provider experiences. Improving the accuracy of data on dual eligibility status by increasing the frequency of federal-state data exchanges is a strong first step in improving how these systems work together.

VII.A.2. Data Exchanges to Support State Buy-in for Medicare Parts A and B

CMS proposes to require all states to exchange Medicare buy-in data with CMS each business day beginning April 1, 2022. If no new transactions are available to transmit on a given business day, the state would not need to send data. **AHIP supports this proposal. We believe it would improve the timeliness of eligibility and enrollment information, support financial security of enrollees, and reduce state Medicaid expenditures over the long term.**

VII.A.3. Exchange of State MMA Data Files

CMS proposes to require all states to send MMA/state phasedown files to CMS each business day beginning April 1, 2022. If no new transactions are available to transmit on a given business day, the state would not need to send data. **AHIP supports this proposal. We believe it would improve the timeliness of eligibility and enrollment information, support financial security of enrollees and reduce state Medicaid expenditures over the long term.**

VIII. INFORMATION BLOCKING

VIII.A. Public Reporting on Information Blocking

CMS proposes to publicly report information about individual clinicians and hospitals who fail to attest that they have prevented practices that unreasonably limit the availability, disclosure, and use of electronic health information, otherwise known as information blocking. We share CMS' concern over existing incentives for some EHR developers and providers to limit the availability of electronic

health information that is key to high-quality, coordinated care and undermines progress toward a more connected health system. **AHIP supports CMS making it transparent which physicians and hospitals are engaged in information blocking in order to discourage the practice and inform consumers.**

IX. Provider Digital Contact Information

To encourage providers to submit their electronic addresses for electronic data exchange into a centralized federal directory of provider information, pursuant to the 21st Century Cures Act, CMS proposes to publicly report those providers who have not added their digital contact information to the National Plan and Provider Enumeration System (NPPES) directory beginning in 2020. As CMS notes, despite being required to do so, many providers have not yet added their digital contact information to the NPPES and digital contact information is frequently out of date. We agree that more needs to be done to encourage providers to update their digital contact information, in addition to the full record, but are concerned that public reporting of missing digital contact information is not enough of an incentive. We believe that self-attestation is insufficient and there is no effective way of validating the information contained in the NPPES on a regular basis. Other health insurance providers would like to rely on NPPES as a reference point for their provider directories, whether for digital contacts or other elements, but find the limitations of NPPES to be too great. **We recommend that CMS consider additional enforcement authorities, such as through the Medicare reporting program requirements and Medicare enrollment and revalidation processes, to ensure that individual providers and facilities routinely update their information, not just digital contact information, and make it publicly available through NPPES.**

X. Conditions of Participation

The proposed rule requires Medicare-participating hospitals, psychiatric hospitals, and critical-access hospitals (CAHs) to send electronic patient event notifications when a patient is admitted, discharged or transferred (ADT) to improve transitions of care between settings and improve patient safety. We support requiring hospitals to send ADT alerts and believe it will be valuable in supporting safe, effective transitions of care between hospitals and community physicians as well as more generally promoting routine exchange of electronic health information. Given that health insurance providers play a significant role in supporting effective transitions of care, patients would also benefit from such information being shared with their health insurance providers. **We recommend that, in addition to sending ADT alerts to another health care facility or to another community provider, a patient's health insurance providers also receive this electronic notification.**

Recognizing, however, that the conditions of participation (COPs) are the most significant penalty under Medicare and Medicaid and can result in removal from the programs we recommend CMS consider the following approaches. CMS should establish a standard within the COPs that states hospitals shall not intentionally inhibit the exchange of electronic information with other providers or patients. Such a standard would make the penalty commensurate with the misconduct, could be implemented almost immediately and would require no exceptions beyond those established by ONC. In addition, as part of Promoting Interoperability, CMS should emphasize interoperability as a means to better coordinate care through a measure that assesses the actual exchange of ADT alerts to

other providers and ultimately to other stakeholders. Hospitals should be able to use existing health information exchange networks, private sector partners, or direct connections to community practitioners to achieve this objective. **We encourage CMS to consider approaches like creating a COP for intentionally information blocking and measuring use of ADT alerts as part of the Promoting Interoperability program.**

REQUESTS FOR INFORMATION

III.C.2.k. Sharing Between Payers and Providers Through APIs

CMS requests feedback on the potential for payers to share information with providers on overlapping populations without patient consent and as part of the treatment, payment and operations (TPO) authority under HIPAA. Health insurance providers share information with providers as part of TPO on a regular basis. For example, health insurance providers furnish large scale data sets and performance reports to accountable care organization, medical homes and as part of bundled payment programs. Moreover, many health insurance providers are data sharing with clinical providers are part of HIEs. Once the TEFCA rule is finalized, we anticipate even greater connections through the "network of network" that is envisioned. **CMS should allow these efforts to unfold and not dictate how health insurance providers connect with providers. We stand willing to work with CMS and providers to develop appropriate standards for data sharing.**

XII. Advancing Interoperability in Innovative Models

CMS seeks comment on how best to promote interoperability among Center for Medicare and Medicaid Innovation (CMMI) model participants and other health care providers as part of the design and testing of innovative payment and service delivery models. CMS has proposed three general principles for achieving this goal:

- Provide patients access to their own electronic health information
- Promote trusted health information exchange
- Adopt leading health IT standards and pilot emerging standards

We agree that CMMI models provide an important lever to advancing interoperability and support integrating the proposed principles on interoperability within new and existing CMMI models.

However, CMS should recognize that some clinical and encounter data may not exist or be difficult to obtain due to the nature of certain risk models. One advantage to full risk models is that alleviates the need for providers to submit bills for individual services, and thus there may not be any encounter data submitted to health insurance providers. Or, even if there is, the coinsurance that might be calculated of the individual service may not reflect the true out-of-pocket cost under, for example, a bundled payment. In some cases, CMMI may need to extend payment and legal waivers to these participants in acknowledgment of the differing circumstances.

Furthermore, we support CMMI working to advance health IT standards through piloting emerging standards. It may make sense to integrate the DRLS work into CMMI demonstrations, and perhaps even expand such efforts to other use cases. CMMI, for example, could test on a multi-payer basis the automation of coverage lookup and prior authorization queries. Moreover, CMMI could integrate block chain into programs such as Primary Cares First to pilot the test standards and technology for a use case such as provider directories and then expand from there to other use cases. CMMI could integrate incentives or requirements into the programs for both health care providers and health insurance providers, and evaluate the resulting accuracy as well as the benefits of the technology.

XIII. Policies to Promote Patient Matching

HIPAA required the adoption of a "unique individual identifier for health care purposes" (UPI) to facilitate accurate sharing of health information by ensuring accurate and timely linking of a patient's health care information across providers and payers. However, due to significant concerns that a single unique identifier would increase risks that PHI would be compromised, Congress prohibited use of federal funds to adopt or assign a unique patient identifier, thus preventing the Department from rulemaking to adopt a UPI standard. In more recent years, Congress directed the Department to examine issues around patient matching and to facilitate private-sector led initiatives to develop a coordinated national strategy to accurately identify patients.

CMS seeks information on how it could leverage its authority to improve patient identification to facilitate improved patient safety, enable better care coordination, and advance interoperability. Accurately identifying and matching patient records across payers and providers is a foundational element to ensuring patient privacy and maintaining data security. In this RFI, CMS acknowledges the considerable stakeholder feedback that the lack of a UPI inhibits interoperability efforts. We understand the constraints in accurately identifying and matching patient records across providers and payers absent a unique, standard identifier. This often includes attempting to match patient identity using a number of data elements to match along different degrees of certainty and still results in overall low match rates within and between entities.

CMS seeks input on specific patient matching solutions and authority for such requirements. Specifically, the Department requests input on requiring a patient matching algorithm, a particular patient matching software, or expanding recent Medicare ID efforts by assigning an identifier to patients enrolled in federally regulated plans.

We recommend the Department not require a patient matching algorithm or a patient matching software solution. Such federal requirements could result in overly prescriptive requirements that constrain iterative improvements in patient matching by the private sector. These solutions would not be able to keep pace with private sector solutions. Further, while assigning identifiers to patients enrolled in Medicare plans, Medicaid and CHIP, and QHPs in the FFEs would expand the number of patients with a CMS-wide identifier, it would not provide a solution for the millions of Americans who gain coverage through their employers or buy individual coverage outside of the FFEs. We do not believe the specific solutions contemplated in the RFI would sufficiently address patient matching challenges or support private sector innovation.

We strongly encourage the Department to continue to facilitate private industry innovation to advance patient matching solutions rather than adopting federal requirements. We believe the appropriate role of CMS and ONC in the area of patient matching is to convene industry stakeholders to collaborate on the goals and means for developing solutions to patient matching. This may include exploring best practices related to patient matching, improving matching criteria, and setting a minimum floor for error rates. For example, CMS should work with ONC to advance standardization of demographic information such as applying the U.S. Postal Service standard to addresses or adding new data elements like email address.

Recently published research in the *Journal of the American Medical Informatics Association* funded by the Pew Charitable Trusts revealed that the standardization of address to the standard employed by USPS would improve match rates by approximately 3 percent, while standardizing last name to the standard used by the Council for Affordable Quality Healthcare would further improve match rates up to 8 percent.14 These findings suggest match rates could be further improved if ONC required use of USPS standards for address within the USCDI and if ONC and CMS required use of USPS address standards by health care organizations. Consistent with Pew's recommendations related to improving patient matching, we further recommend CMS work with ONC to require other demographic information such as email address, mother's maiden name, or health insurance provider identification number in order to further improve match rates.

AHIP further recommends that ONC or CMS-convene a working group to identify minimum assurance rates which would vary by setting. For example, the level of assurance of accurate patient matching needed for administrative or payment information would be lower than the level of assurance needed for treatment. We additionally recommend CMS adopt a safe harbor for entities that follow best practices or meet these assurance rates.

Industry should have the flexibility to continue to iterate solutions to identify and match patient records. Building on best practices or minimum assurance rates, such solutions may include leveraging patient authorization, improving existing processes like copying and storing a patient's ID card at the provider's office, or public-private partnerships like those that have successfully solved person-matching issues in other industries such as the airline industry and TSA security check process. We believe CMS' role is to facilitate and set a floor for such innovation, but not restrict private sector solutions.

XI. Advancing Interoperability Across the Care Continuum

CMS requests comment on how it can more broadly incentivize the adoption of interoperable health IT systems and use of interoperable data across settings such as long-term and post-acute care, behavioral health, health care settings serving dual eligible and home and community-based services (HCBS) recipients. CMS seeks comment on needed measure development work and quality improvement efforts focused on assuring individuals receive needed services across the care

---

[14] Shaun J Grannis et al., "Evaluating the effect of data standardization and validation on patient matching accuracy," Journal of the American Medical Informatics Association 26, no. 5 (May 2019): 447–456, https://doi.org/10.1093/jamia/ocy191

continuum and that their services are coordinated, as well as the applicability and feasibility of measure concepts for post-acute care, behavioral health, and HCBS.

Promoting interoperability among post-acute care providers will increase efficiency and promote safety as patients move between health care settings. Health insurance providers have noted several challenges in obtaining data from long-term and post-acute care providers for the purposes of reporting quality measure data. Increased data sharing among these providers will lead to more valid measure results. We recommend that CMS work closely with post-acute care providers to determine what data elements can be feasibly exchanged and use that information to inform future measure development. **We also recommend that future interoperability requirements for post-acute care providers be aligned to the extent possible with those of payers, providers, and health IT developers in terms of technical standards and methods of exchange. AHIP supports efforts to promote interoperability and efficient health IT use across the care continuum.**