June 3, 2019

Centers for Medicare & Medicaid Services
Department of Health and Human Services
Attention: CMS–9115–P
P.O. Box 8016
Baltimore, MD 21244–8016

Office of the National Coordinator for Health Information Technology
Attention: RIN 0955–AA01
Mary E. Switzer Building, Mail Stop: 7033A
330 C Street, S.W.
Washington, DC 20201

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

> ***Re: Comments to 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;***
>
> ***Comments to RIN 0955–AA01; 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program.***

Dear Sir or Madam:

The Medicaid Health Plans of America (MHPA) appreciates the opportunity to comment on the proposed rules issued by the Centers for Medicare & Medicaid Services (CMS) and the Office of National Coordinator for Health Information Technology (ONC) intended to work together to facilitate access to electronic health information for patients and to help solve issues related to interoperability. MHPA is the national trade association representing 94 private-sector health plans that contract with state Medicaid agencies in 37 states plus the District of Columbia to provide comprehensive, high-quality health care to more than 23 million Medicaid enrollees in a coordinated and cost-effective way. Our member plans offer comprehensive, coordinated care that supports the health care needs of Medicaid beneficiaries while also managing costs for our state and federal partners.

MHPA supports CMS and ONC's efforts to advance the policies and goals of the MyHealthEData initiative to empower patients, including Medicaid beneficiaries, by breaking down the barriers that impede patients' ease of access to their electronic health care information. We agree that facilitating patient access to their own health care information can encourage patients to take charge of and better manage their health care and help improve the patient experience and health outcomes. We also believe that Medicaid managed care plans are important partners in this effort and that facilitating patient access to their own electronic health information is in the best interests of patient health.

MHPA also recognizes and supports that technology is an important, valuable tool for patient access to their health information and that the lack of interoperability can act as a barrier for patient access to this information. We support CMS and ONC's intent to remove these barriers for patients and to set a standard that requires no special effort for patient access to this information.

However, we also believe that a patient's electronic health information is personal, contains sensitive information, and should be accessible and exchanged in a way that protects and prioritizes the privacy interests of the patient. We are greatly concerned that many of the requirements established by these proposed rules could result in an approach that is rushed, unsustainable, and puts patient information at risk while creating additional pressures, burdens, and costs on our overburdened health care system. In short, we believe the compliance undertaking required by the proposed rules is considerable and the short implementation timeframe is overly aggressive with an unacceptable level of risk.

To facilitate a smooth pathway toward interoperability across health care programs and delivery systems, including Medicaid, we recommend that CMS and ONC consider a phased-in approach for interoperability with the same focus and goal of patient empowerment, but that is flexible and allows for assessments, analyses, and adjustments at designated check-in points over time and is informed by a broad spectrum of stakeholder engagement and feedback. Alternatively, at a minimum, we recommend that CMS and ONC delay the effective date for implementation of the requirements under these proposed rules.

Our specific comments on aspects of the proposed rules are as follows:

Availability of Electronic Health Information through a Standardized Application Programming Interface

MHPA appreciates the overarching goal of these proposals that lay the groundwork for a pathway for every American, without special effort or advanced technical skills, to be able to access, see, obtain, and use their own electronic health information. Third-party consumer applications (commonly referred to as "apps") are important and valuable tools for accessing information that can be convenient and expedient. This technology has been instrumental in revolutionizing numerous industries, including health care, and has changed consumer expectations about what is standard practice. In the health care arena, it has presented incredible opportunities for engagement and collaboration between and across multiple parties, including patients, caregivers, health care providers, health plans, and payers. We appreciate that standardizing requirements to facilitate sharing of electronic health information through

application programming interface (API) continues this important journey toward interoperability as envisioned in the 21st Century Cures Act.

However, given the sensitivities related to personal health information, technology related to the accessibility and transferring of such information can also present high risk if not thoughtfully considered for its potential impact across stakeholders and if not implemented with appropriate safeguards and protections. In relation to these proposed rules, we do not believe sufficient consideration has been given to the interests of patient privacy and data security and that the rush to comply with these standards may result in unnecessary risks for data breaches, exposure, and data misuse, as well as result in a significant expenditure of resources by stakeholders.

Data Standardization

MHPA believes that data standardization is a necessary and critical step in furtherance of interoperability. We appreciate the steps taken by CMS and ONC to coordinate their efforts to help guide the development of an infrastructure and system that supports the exchange of electronic health information.

However, we do not support the proposed standards given the magnitude of the changes and the required timeframe for their adoption. For example, we recommend that CMS and ONC allow for additional time for input from stakeholders, including health plans, to better inform the data elements that best represent a patient's health journey – including both clinical and non-clinical data points. We also recommend that there should be enough time allowed for stakeholders to become familiar with and support compliance with the new standards.

Privacy & Security of Electronic Health Information

MHPA believes the current proposals do not appropriately consider or sufficiently address the potential risks related to the privacy and security of patient health information to be electronically transferred through APIs. We agree with CMS that when patient health information is in play it "requires appropriate diligence to protect the individual's privacy, such as their current and past medical conditions and care received." However, we do not believe that current API technology includes the cybersecurity and authentication features that is necessary to protect this sensitive information.

We believe the potential for risk to patient health information presented by moving forward prematurely, meaning before the implementation of appropriate safeguards and protections, is simply too great. In other words, third-party access to patient health information, absent sufficient privacy and security protections, presents an unacceptable risk of misuse of this sensitive information. To better protect patient health information, we urge CMS and ONC to slow down the implementation timeline and allow for a more thorough assessment of potential cyber threats and the identification of a path forward that begins with patient privacy and security as a foundational principle.

Further, we are concerned with the proposed rule's requirement that places the burden, costs, and liability on health plans to "to implement, test, and monitor an openly published API that is accessible to third-party applications and developers." We do not believe that plans and

providers should be responsible for ensuring that a third party complies with the privacy and security obligations the third-party developer is required to meet under state and federal law. As health plans, we are responsible for the provision of comprehensive, high-quality health care to our Medicaid enrollees; we are not in the business of compliance monitoring for third-party health information technology vendors. Therefore, we urge CMS and ONC to explicitly address that the election of sharing through the API to the third-party app would be patient initiated and that the privacy and security of the electronic health information becomes the responsibility of the third party to which it is transferred on request of the patient. In addition, we recommend CMS and ONC consider a third-party application vetting process or provide a CMS or ONC-vetted list of third-party apps that are "approved" to which patient-requested information could be transferred.

We appreciate and support efforts to help inform and educate patients about the impact of the proposed changes on access to their electronic health information, including potential privacy risks associated with data sharing. In furtherance and in support of efforts to promote transparency and encourage patient engagement, we urge CMS to continue to work with stakeholders, including Medicaid health plans, to consider how educational efforts could be uniquely tailored to specific subpopulations, particularly given the need for special considerations when attempting to engage with vulnerable populations such as Medicaid beneficiaries. In particular, we note that language barriers, varying levels of health literacy, and individual comfort with technology may be best addressed via distinct, yet aligned, educational strategies depending on individual needs. To most effectively implement this approach and given the breadth of educational efforts required, MHPA recommends that CMS amend or revise the current language in its proposed rule that seems to place sole responsibility on Medicaid managed care organizations for the education of Medicaid enrollees about the potential privacy and security risks associated with data sharing. We believe patients would benefit from the delivery of these messages through multiple channels and recommend that CMS clarify and state explicitly that the responsibility for education of consumers is to be addressed across stakeholders, including API vendors.

Operational Issues

MHPA notes there are considerable administrative and operational challenges presented by these proposals. Given the required changes to policies and processes, we caution CMS and ONC that the timeframe for implementation (i.e., July 1, 2020 for Medicaid health plans) is unrealistic given the multi-faceted requirements related to assessing and understanding the technological requirements, implementing these requirements, and then executing on these requirements as a new standard of business operations. Simply, we believe the proposals do not allot sufficient time to meet these requirements nor even to discuss or develop a strategy to address these requirements.

Most notably, we would like to underscore for CMS and ONC the operational challenges required for the development of a security strategy and control architecture for API data sharing. While we fully support the empowerment of patients and the removal of barriers to patients accessing their own health information, we also view ourselves as stewards of our patients' health information. As stewards, we are entrusted with protecting the privacy and security of a patient's electronic health information and would urge CMS and ONC to allow sufficient time

for health plans to develop a security strategy that provides for sharing of electronic health information with APIs without putting patient health information at increased cyber risk.

We also note that some health plans may currently operate databases that need time to be modernized in order to meet API data sharing requirements. New system adoptions require time, funding, and workforce engagement. We do not believe the implementation timeframes account for system and staffing demands on health plans to develop expertise in these standards and to fully implement them into standard business operations.

In addition to the time and resources required to implement such changes, we also believe that there remain important elements in support of interoperability that are still in flux and should be finalized before being required under this proposed rule. For example, the proposed rule would require the participation of Medicaid health plans, among others, in trusted exchange networks meeting specific criteria. However, Draft 2 of the Trusted Exchange Framework and Common Agreement (TEFCA) was just released on April 19, 2019, with changes from Draft 1 released in 2018, proposing a common set of principles, terms, and conditions to support the development of a Common Agreement to better enable nationwide exchange of electronic health information across disparate health information networks.

And, finally, we have concerns that the implementation timeline simply does not allow health plans to understand and seek clarity on the interplay between federal and state laws related to the access and availability of patient electronic health information nonetheless develop and effectively implement a compliance plan in a timely manner.

Types of Electronic Health Information - Availability

Medicaid managed care plans are important partners in patient health. MHPA supports access to health information that is appropriate to coordinate care that is in the best interests of patient health, including a patient's own health information, such as diagnoses, and health plan coverage policies, such as cost-sharing requirements.

- *Published Provider Directory and Drug Benefit Information*

We support patient access to information related to their health plans' coverage policies such as a list of in-network providers and the prescription drugs that are covered on formulary. We also note that this information is typically already available and accessible either online or provided as a hard copy by many of our health plan members. To avoid unnecessary duplication of effort and the incurrence of additional avoidable costs, MHPA recommends an explicit exemption for health plans that are already providing this information in the manner that aligns with the requirements under the proposed rule.

- *Patient Claims and Encounter Data*

While we support patient access to their claims and encounter data, we have concerns about the proposed 1-day turnaround time for making claims and encounter data available to patients. In addition to potential system and process changes, health plans will most likely need to modify provider contracts to meet this requirement. We believe that attempts to modify provider contracts by the January 1, 2020 and July 1, 2020 time frames would be a significant

challenge and place additional administrative burdens and costs on clinicians who most likely have contracts with multiple plans and payers.

- *Pricing and Proprietary Information and Trade Secrets*

MHPA does not support the inclusion of pricing and proprietary information or trade secrets as types of information to be required for data sharing.

We believe that including specific price information within the scope of required data sharing could lead to unintended, anti-competitive consequences. Health plans devote time and resources to ensuring that patients receive the best and most cost-effective care possible. Provider reimbursement rates, contracting strategies, prior authorization and care management programs, and formulary development policies are proprietary information that health plans have developed to provide the best value to patients. We do not believe that sharing this competitive information between or across plans furthers the goals of care coordination and the potentially anti-competitive effects could drive up overall costs and stifle innovation.

Proprietary information and trade secrets include business strategies, operations, financial information, studies, processes, and other information regarding the health plan's business that the health plan has taken reasonable measures to keep secret and the health plan derives independent economic value, actual or potential, from the information not being generally known and not being readily ascertainable.

Accordingly, MHPA recommends that pricing and proprietary information and trade secrets should not be designated as electronic health information for purposes of this proposed rule and that CMS should not require that health plans to share pricing or proprietary information or trade secrets with third parties via API.

Provider Access to Electronic Health Information and Care Coordination

Representing health plans responsible for the delivery of comprehensive, high-quality health care to more than 23 million Medicaid enrollees, we know first-hand that coordinated care can result in better health care quality and better health outcomes. We applaud CMS and ONC's efforts to embrace and support technology as a tool to connect the disparate components of our health care system and remove barriers to ensuring that patients and health care providers have more comprehensive access to patient health records and information. We have several recommendations related to the proposed rules' requirements specific to care coordination and the promotion of information and data exchange.

First, we recommend that a distinction be made between information that is collected by a health plan and clinical information collected by a health care provider. Health plans do not necessarily maintain electronic health records – these are most likely maintained by health care providers – and generally collect and maintain information that is needed to meet health plan centric business requirements such as paying claims and submitting encounters. We believe that a distinction between non-clinical health plan information and clinical information may present opportunities to smooth the pathway toward interoperability with policies that could apply to one set of information and not the other.

Second, we believe the proposed requirement for health plans to use the Trusted Exchange Network framework to allow for broader operability does not provide enough detail in the framework to establish these connections. As noted earlier in this letter, Draft 2 of the TEFCA was just released on April 19, 2019 and has not been finalized. Given the interest of CMS and ONC to move forward quickly on interoperability, however, we also raise for consideration whether the framework provided by TEFCA, once finalized, is better positioned to provide a pathway to broader interoperability than the establishment and support of APIs.

And, finally, we would like to note that regulatory barriers remain for health information exchanges to operate and seamlessly share patient information. For example, the so-called Part 2 rules—the Confidentiality of Substance Use Disorder Patient Records rules – prohibit certain entities from disclosing any information that would identify a person as having or having had a substance use disorder unless that person provides written consent. To meet the requirements of Part 2, covered entities must obtain patient consent before disclosing Part 2 patient-identifying information, including to a health information exchange. We encourage CMS to consider how to address such barriers to care coordination and health information exchange in future rule-making.

Improving the Medicare-Medicaid Dually Eligible Experience by Increasing the Frequency of Federal-State Data Exchanges

CMS proposes to update the frequency requirements for states to submit the required MMA file data to CMS on a daily basis starting April 1, 2022. MHPA supports CMS's efforts to increase data sharing frequency and respectfully requests clarification if this proposal encompasses a reciprocal daily response from CMS to the states. Further, we seek clarity on whether the proposal provides for Medicaid managed care organizations to have daily access to the MMA data for the purposes of benefit and care coordination between the Medicaid and Medicare programs.

Information Blocking

In furtherance of transparency and coordination of care, we support policies that prevent health care providers from inappropriately restricting the flow of information to other health care providers and payers. While we are cognizant and supportive of the important protections in place for patient privacy through the Health Insurance Portability and Accountability Act (HIPAA) and additional, often more restrictive, state laws, we are uncertain about the interplay between the proposals related to information blocking and current federal and state privacy laws. Therefore, we seek clarity from CMS and ONC that health plans would be not be subjected to data sharing restrictions and penalized for not sharing or blocking data if they cannot, under other applicable laws, provide the information.

We also believe the definition in the ONC proposed rule for "Health Information Network or HIN" at § 171.102 - Definitions is overly broad and request further clarification and greater specificity about the activities that meet this definition.

Implementation Timeline

MHPA has serious concerns about the proposed implementation timeline and its potential to force the implementation of an approach to interoperability that is premature and could lead to unnecessary additional costs on the health care system. MHPA believes the implementation timeframe is unrealistic and impractical given the numerous administrative, operational, policy, and process changes needed for compliance. For example, a foundational component of this proposal is that Medicare Advantage organizations, qualified health plan issuers in the Federally-facilitated Exchange, and Medicaid managed care plans meet the proposed requirements to make patient claims and other health information available to patients through third-party applications and developers that includes implementing, testing, and monitoring an openly-published Health Level Seven (HL7®) Fast Healthcare Interoperability Resources (FHIR®)-based APIs. Compliance with this one component is complex and multi-faceted with potential changes required to a health plan's infrastructure, systems, policies, processes, and its workforce. We note that the compliance deadlines of July 2020 for Medicaid health plans and January 2020 for other plans are only 13 and 7 months away, respectively, from the revised deadline for request for comments for these proposed rules. We do not believe this timeframe is realistic or fair.

We also caution CMS and ONC that an approach that prioritizes the speed of implementation over a thoughtful, more deliberate approach is likely to cost more in the long-run. We urge CMS and ONC to allow for the necessary time to research, develop, test and implement the proposed requirements.

Accordingly, we believe that a delayed implementation or a phased-in approach (e.g., over a period of 5 years) is the preferred pathway to interoperability. Such an approach would allow sufficient time for course corrections in standards and policies prior to stakeholders investing significant resources – both financial and workforce -- into changes to their infrastructure, systems, policies, and processes. We acknowledge that a more measured approach may take more time upfront; however, we believe such an approach is more likely to build a foundation for the interoperability of electronic health information across health care programs and delivery systems that is capable of long-term sustainability and future success.

Medicaid Program Sustainability

In furtherance of the efficiency, effectiveness, and sustainability for administration of the Medicaid program, we recommend that the cost of compliance with the multitude of requirements, including but not limited to system changes, the development and implementation of new policies and processes, worker training, and monitoring and reporting, be recognized within the framework of actuarially sound rates.

Requests for Information - *Policies to Improve Patient-Matching*

We appreciate the opportunity to provide comments in response to the request for information to help inform future rule-making on patient matching. MHPA supports patient information verification efforts as critical steps in furtherance of patient safety. To allow for flexibility and choice and promote innovation, MHPA recommends broad support for initiatives to verify patient data and identities without restrictions to the use of a particular patient matching software solution, vendor or algorithm.

*   *   *   *

Thank you for the opportunity to provide comments on these proposed rules. Our member plans are committed to serving Medicaid beneficiaries and are available to assist you as you consider the applicability of this rule to the Medicaid program and Medicaid health plans in particular. Should you need any additional information or seek further clarification on our comments or recommendations, please feel free to contact me at sattanasio@mhpa.org.

Sincerely,

Shannon Attanasio

Shannon Attanasio
Vice President, Government Relations and Advocacy