June 3, 2019

Seema Verma
Administrator
Centers for Medicare and Medicaid Services
U.S. Department of Health and Human Services
200 Independence Ave., SW
Washington, DC 20201

Submitted electronically via www.regulations.gov

RE: Interoperability and Patient Access Proposed Rule (CMS-9115-P)

Dear Administrator Verma:

On behalf of more than 100,000 specialty physicians from 15 specialty and subspecialty societies, and dedicated to the development of sound federal health care policy that fosters patient access to the highest quality specialty care, the undersigned members of the Alliance of Specialty Medicine (the "Alliance") appreciate the opportunity to comment on the agency's *Interoperability and Patient Access* proposed rule. The Alliance applauds both CMS and Office of the National Coordinator for Health Information Technology (ONC) for its cross-agency effort to seriously advance interoperability among health care providers, payers, and patients, and to help patients become more engaged partners in their care by enhancing access to data.

Both rules aim to stimulate game-changing innovation that is intended to minimize errors, improve care coordination, reduce physician burden, lower costs, and enhance consumer experience. The Alliance strongly supports these goals and has no doubt that the CMS rule will improve patient access to information and further engage patients in their health care. However, the Alliance also has serious concerns that if this data is unleashed too rapidly and without adequate standards, parameters, and context, it will be uninterpretable to patients and at considerable risk for misuse. If the goal is to make patients better healthcare consumers, then it is critical for both CMS and ONC to carry out these reforms carefully and gradually to ensure that data can be shared with patients in a meaningful and usable format. If the infrastructure is not first in place to ensure these protections, this surge of data will simply overwhelm patients and the physicians who care for them and potentially be misapplied in ways that impact coverage, access to care, and the physician-patient relationship.

That being said, the Alliance appreciates that this rule takes a distinct approach by focusing on the role of health plans in terms of advancing data access and interoperability. While payers are certainly not the only source of healthcare data, they are in a unique position to provide enrollees with a more complete picture of their claims and encounter data and therefore play an important role in ensuring the accessibility of patient data. Historically, many of CMS' health IT and interoperability efforts have been focused strictly on clinicians and hospitals. We appreciate that this rule aims to ensure that all health care industry stakeholders, including payers, are working together to advance health information exchange.

Listed below is an executive summary of our comments, followed by a more detailed set of comments on specific proposals that will likely have the biggest impact on Alliance members.

Executive Summary

- **Patient Access to Data Through Open APIs**
  - The Alliance strongly urges CMS to more carefully evaluate the potential implications associated with making data so easily accessible and transferable, including risks related to information overload, data security, and increased physician burden.
  - The federal government also must carefully re-evaluate the reach of HIPAA in the context of modern data exchange and sets clear parameters for the appropriate use of data by third-party entities. Similarly, CMS' regulatory policies, including physician payment policies, must evolve to reflect the additional demands that will placed on physicians.
  - Federal agencies must clearly educate patients on the implications of sharing their data with third-party entities that are not HIPAA non-covered entities and the potential for data to be misused in ways that can impact coverage, access to care, and interfere with the physician-patient relationship. HHS also must provide clear guidance to physicians about their obligations under this shifting landscape.
  - CMS should require payers to provide prior authorization requirements to patients and physicians as part of this data access proposal.
  - CMS should prohibit payers from using these proposals to place additional contractual demands on physicians.
  - We request that CMS reconsider the "one-day" requirement as plans and clinicians adjust to new API and other data access policies, as well as the implementation deadline of January 1, 2020.
- **RFI on Information Sharing Between Providers and Payers Through APIs**
  - CMS should clarify how it plans to support the integration of administrative data made available by health plans with clinical data that may be housed in an EHR so that patients and clinicians have a more complete picture of the patient's health and medical care.
  - CMS should clarify how it plans to protect patients from health plans misusing this data to limit coverage or access to care**.**
- **Health Information Exchange and Care Coordination Across Payers**
  - The Alliance supports this proposal in concept, but raises multiple questions about CMS' implementation strategy.
- **Care Coordination Through Trusted Exchange Networks**
  - CMS should address the potential for plans to shift some of the costs of participating in these networks to patients and providers.
- **Improving the Dual Eligible Experience by Increasing Frequency of Federal-State Data Exchanges**
  - The Alliance supports requiring more frequent exchanges of this data so long as this requirement does not impose additional reporting requirements on clinicians.
- **Information Blocking**
  - We remind CMS to ensure that all clinicians who exempt from the PI category or otherwise not obligated to attest to the prevention of information blocking statements are not publicly portrayed as "bad actors." We also request that CMS consider including

a disclaimer on Physician Compare explaining why some clinicians are not required to make these attestations.

- **Provider Digital Contact Information**
  - We request that CMS clarify what it means by "digital contact information" and provide more concrete examples and/or illustrations. We also request that CMS provide updated educational materials on the role of the National Plan and Provider Enumeration System (NPPES) and these new requirements, if finalized.
  - We support positive incentives, rather than public shaming or other disincentives, to promote accurate and up-to-date digital provider contact information in the NPPES.
- **Revisions to the Conditions of Participation (CoPs) for Hospitals and Critical Access Hospitals**
  - We support the intent of this proposal, but recommend that CMS focus on building the existing exchange infrastructure rather than layering additional requirements for hospitals to participate in Medicare.
- **Advancing Interoperability in Innovative Models**
  - We support the testing of innovative solutions to promoting interoperability so long as they account for provider costs associated with the implementation of these more standardized systems.
- **RFI on Policies to Improve Patient Matching**
  - We urge CMS to evaluate potential solutions carefully to ensure they do not exacerbate current challenges and lead to more errors or increased administrative burden.

Detailed Comments

Patient Access to Data Through Open APIs

CMS proposes to require Medicare Advantage (MA) organizations, state Medicaid and CHIP FFS programs, Medicaid managed care plans, CHIP managed care entities, and Qualified Health Plan (QHP) issuers in Federally-Facilitated Exchanges (FFEs) to make a variety of patient claims and clinical data available to patients through an openly accessible HL7® FHIR®-based Application Programming Interface (API). The types of data that plans would have to make accessible to patients, at a minimum, include:

- Adjudicated claims (including cost);
- Encounters with capitated providers;
- Provider remittances;
- Enrollee cost-sharing;
- Clinical data, including laboratory results, only if the plan "receives and maintains this data as part of its normal operations;"
- Formulary information (for MA Part D drug plans) or information about covered outpatient drugs and preferred drug lists (for Medicaid/CHIP plans); and
- Provider directory data

The plan would have to make this data available through the API within one business day after a claim is processed or the data is received by the payer. Patients would then be able to access this data through third-party applications of their choosing. Under this proposal, plans would be required to build and make available these APIs by January 1, 2020.

The Alliance recognizes the value of APIs in terms of greater patient empowerment over healthcare decisions, establishing points of communications between systems and stakeholders that allow for the more efficient exchange of information, and enhancing interoperability. In theory, it would be great if

patients could download an application to their smartphone, access all of their health information in one place, and then share that information with providers and caregivers with the click of a button. However, in reality, the process is not that straightforward. ***We strongly urge CMS to more carefully evaluate the potential implications associated with making data so easily accessible and transferable, including risks related to information overload, data security, and increased physician burden.*** Some of these implications are discussed below.

As a result of proposals in this rule, as well as other recent policy decisions, patients will have access to an unprecedented amount of information, which will be challenging to manage, decipher, and prioritize. As information is made more accessible, patient demands and expectations of clinicians also will rise. Already, patients receiving information through APIs may contact a clinician with inquiries before the clinician even gains access to the information. This changing dynamic will not only overload clinicians with potentially irrelevant information, but place unprecedented pressure on clinicians to respond to and mange patient inquiries. Furthermore, as patients gain access to a wider array of information, their inquiries are expected to focus on not only clinical topics, like lab values and test results, but also claims and cost-sharing information over which the clinician may have little direct control. Finally, we hope that third-party application developers will seek out clinical expertise as they build products that attempt to present complex health data in a patient-friendly format, which will put additional demands on clinicians. Many physicians already feel that their time with the patient has been depleted by a variety of administrative and EHR-related disruptions and these new demands will further disrupt the patient-physician relationship. ***As patients gain more access to their data and become more engaged partners in their care, it is critical that CMS' regulatory policies, including physician payment policies, evolve to reflect the additional demands that will placed on physicians, including the time and resources needed to respond to patient inquiries and provide guidance to application developers.***

With these concerns in mind, we request that the proposed list of data types that plans must make available through APIs focus on information that is truly relevant to patients and useful to clinicians treating those patients. One piece of information that both patients and clinicians are often missing, and which interferes with timely access to care, is a clear explanation of prior authorization requirements. ***The Alliance requests that CMS require payers to provide prior authorization requirements to patients and physicians as part of this data access proposal.***

Given our earlier concerns about information overload, we appreciate that CMS is taking steps to at least ensure standardization by proposing to require that plans conform to the same API technical standards as those proposed for certification in the ONC proposed rule, and to rely on an aligned set of content and vocabulary standards for clinical data classes (i.e., the United States Core Data for Interoperability standard (USCDI v1)). At the same time, we note that plans that do not receive and maintain clinical data (e.g. clinical notes, imaging results, and lab results) as part of their normal operations would be under no obligation to make such data available to patients through the API. ***Given the importance of clinical data, especially to physicians who are managing the care of a patient, we request that CMS clarify how it plans to support the integration of administrative data made available by health plans with clinical data that may be housed in an EHR so that patients and clinicians have a complete picture of the patient's health and medical care.*** If APIs provide access to little more than what is already included in a payer's Explanation of Benefits, this initiative will bring little value to physicians and will further confuse patients. Both physicians and patients need access to clinical data to ensure they can make qualitative decisions based on a complete picture of the patient's health and care.

Another major concern of the Alliance is that patients might not understand that many entities that currently collect personal health information, such as fitness trackers or apps used to regulate blood pressure, fall outside the scope of the HIPAA, which could put their health data at risk. Even if patients understand these risks, it may be challenging for them to determine whether a healthcare application allows them to securely download, view, store, and share their data.   The Alliance appreciates that CMS proposes to require payers to conduct routine testing and monitoring of APIs to ensure they function properly and have appropriate privacy and security features. We also appreciate HHS' clarification that "covered entities," such as payers and providers, would not be responsible under HIPAA for the security of protected health information (PHI) once it has been received by a third-party application chosen by the patient.

However, these policies only address half of the problem. They do not address the fact that an increasing number of organizations, which are not subject to the same rules concerning the protection of PHI as are other covered entities, are now collecting, storing, and transmitting health data. The ONC recognized, as early as 2016, that there is a "lack of clear guidance around consumer access to, and privacy and security of, health information collected, shared, and used by non-covered entities."[1] With no consistent standards for the protection of health information for these non-HIPAA covered entities, patients face a high risk of having their health data exposed, stolen, or misused. ***Therefore, the Alliance believes that the time has come for the federal government to carefully re-evaluate the reach of HIPAA in the context of modern data exchange. Privacy and security protections for health information must keep up with the pace of technology and the influx of non-covered entities now managing ePHI.*** We are supportive of the direction ONC seems to be taking in the updated draft of its Trusted Exchange Framework and Common Agreement, which requires non-HIPAA entities, who elect to participate in exchange, to be bound by certain provisions that align with safeguards of the HIPAA Rules. The Alliance agrees with ONC that this will bolster data integrity, confidentiality, and security, which is necessary given the evolving cybersecurity threat landscape. The Alliance expressed these sentiments in its comment letter to the ONC, as well.

The Alliance is also concerned that payers and third-party entities may inappropriately use aggregated data gathered from patient's records to draw potentially inaccurate and unreliable conclusions about clinician performance or that insurers may use patient health information collected through apps to limit/exclude coverage for certain services. ***While these might not be HIPAA issues, it is equally important that the federal government set parameters for the appropriate use of data by third-party entities. We believe that ONC should establish an appropriate security controls framework for interoperability and data sharing, including a strategy to ensure that third-party apps properly authenticate for EHI use and do not improperly modify or use a patient's medical record.***

We appreciate that CMS proposes specific requirements on payers to ensure enrollees understand how to protect their PHI, important things to consider when selecting a third-party application, and where they can lodge a complaint if they believe if they have been subject to unfair or deceptive actions or practices. However, we believe that federal agencies also have an obligation to assist with education and to set standard terms and conditions that would make it very clear to patients what they are agreeing to, how their information could be used, which organizations are required to comply with HIPAA and which are not. These duties should not fall on the shoulders of clinicians. It is also important

---

[1] Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA. Office of the National Coordinator for Health IT, 2016.

for federal agencies to educate the physician community about these new risks, as well as what role and obligations the physician has in terms of making data available, authenticating the identity of requestors of data, and otherwise authorizing access to data. ***In summary, it is critical that federal agencies work together to conduct an aggressive educational campaign to clearly explain to patients the implications of sharing their data with third-party entities that are not non-covered entities and the potential for data to be commoditized or otherwise misused in ways that can impact coverage, access to care, and interfere with the physician-patient relationship. It is equally important that federal agencies provide clear guidance to physicians about their obligations under this shifting landscape.***

The ONC rule restricts physicians from charging patients to access their health information through APIs. However, neither the ONC or CMS rule dictate the same requirement for health plans, which raises the question of who will absorb the additional costs to plans for complying with this new mandate. We are concerned that health plans will pass down costs and other requirements to their network physicians through burdensome and potentially coercive contractual clauses. For example, elsewhere in this rule, CMS proposes to require that health plans participate in a trusted exchange network to improve interoperability and allow for the nationwide exchange of data. Using narrow network tactics, a payer may force a physician to participate in this exchange to ensure that the payer has access to the physician's clinical information, and require the physician to take on the cost of doing so. Narrow networks are a serious problem for specialty physicians and these requirements could result in payers have even more control over physicians and further limiting patient access to critical specialty care. ***We request that CMS prohibit payers from using these proposals to place additional contractual demands on physicians.***

The Alliance also has concerns about the requirement for plans to make data available through an API within one business day after a claim is processed or the data is received by the plan. Since a payer's ability to provide data within one business day will depend on providers submitting the data on a timely basis, we are concerned that plans will put undue pressure on network regarding the submission of claims and encounter data to comply with API requirements. We remind CMS that most clinicians are already submitting this data in as timely a manner as possible since it is tied to reimbursement. ***While we appreciate the need for timely access to data, we request that CMS reconsider the "one-day" requirement as plans and clinicians adjust to new API and other data access policies.***

In this section of the rule, CMS also proposes that through these open APIs, MA plans, as well as state Medicaid and CHIP Plans (FFS and managed care), must provide the general public with access to a directory of the plan's network of contracted providers, including provider's names, addresses, phone numbers, and specialties. These plans would be required to update provider directory information available through the API no later than 30 calendar days after changes to the provider directory are made. ***The Alliance supports this proposal. Although provider directories are already often available to enrollees and potential enrollees in hard copy form or on a plan's website, this proposal addresses the content and format in which such directories would have to made available via APIs and would ensure this information is more easily and broadly accessible through interoperable technology.***

Given all of the concerns raised above, the Alliance requests that CMS reconsider the implementation deadline of January 1, 2020. CMS acknowledges there is substantial work to be done by health IT developers and their customers to build and deploy technology to support these proposals. API technology and associated policies related to the sharing, security, and privacy of health care data are complex and must be deployed correctly rather than rapidly. As we discuss in our comment letter to

ONC, we are also concerned that the Information Blocking exceptions do not provide strong enough protections to prevent health plans, EHRs, or API-developers from passing on the costs of implementing this technology to providers. If implementation is rushed and EHRs and health plans are required to adopt open APIs before it is feasible, these costs may be heightened.

RFI on Information Sharing Between Providers and Payers Through APIs

CMS seeks comment, for possible consideration in future rulemaking, on the feasibility of providers being able to request from payers a download on a shared patient population, and whether they could leverage the APIs proposed in this rule for this purpose. CMS clarifies that it does 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 to instead specify a new and additional mechanism by which to share health information as directed by the individual, through the use of API technology and in compliance with all existing privacy and security laws.

The Alliance appreciates that this request for feedback focuses on the provider since most of the proposals in this rule seem to focus on enhancing *patient* access to health information. Although CMS talks about how the API and other proposals could also benefit clinicians (e.g. by allowing them to integrate claims and encounter information with EHR data), it offers no clear mechanism that would ensure that clinicians could easily access health plan data on a shared patient population all in one spot. Patients undeniably have a right to their own data, and the Alliance supports efforts to better enable patient access to data. However, it is also critical that physicians overseeing the care of a patient have easy and direct access to a patient's history—both in terms of clinical and administrative data. If mechanisms were in place to facilitate payers sharing data with a clinician's EHR ahead of time, it could save time during appointments, reduce duplicative screenings and assessments, minimize repeated utilization reviews, streamline prior authorization processes, and ultimately improve the quality of patient care. Direct access to this information would also benefit providers in Accountable Care Organizations (ACOs) and other shared accountability models that require taking on risk since it would provide a more complete picture of their patient population's needs and help them to better budget for appropriate resources. ***The Alliance supports CMS' pursuit of policies that would encourage payers to use the proposed API infrastructure as a means to exchange information with clinicians on a shared population of patients. As we raised earlier, we request that CMS clarify how it plans to support the integration of administrative data made available by health plans with clinical data that may be housed in an EHR so that patients and clinicians have a more complete picture of the patient's health and medical care.***

At the same time, we are concerned about payers gaining unprecedented access to clinical data. ***We request that CMS clarify how it plans to protect patients from health plans misusing this data to limit coverage or access to care.***

Health Information Exchange and Care Coordination Across Payers

CMS also proposes that a minimum set of data follow the patient as they move from plan to plan. Although payers and health plans currently may exchange information for the purpose of the care coordination, this proposal would require plans to gather and exchange all patient information in one place. A payer must, if asked by the beneficiary, forward his or her information to a new plan or other entity designated by the beneficiary for up to 5 years after the beneficiary has disenrolled from the plan. Impacted plans must exchange, at a minimum, the data elements associated with the <u>USCDI v1 data set</u>

standard at the patient's request. The assumption is that the patient could then access this aggregate data—including their treatment history, prescription drug history, and all the providers who have billed for services for that patient— via the current plan's API. However, CMS does not specify the means of exchanging this data at this time (i.e., plans could use APIs, but are not required).

The Alliance supports this proposal in concept since it promotes data exchange between plans and the creation of more longitudinal patient records that, if ultimately shared with clinicians, could result in greater efficiencies in care. *As patients move throughout the healthcare system, in particular from payer to payer, they should be able to maintain access to their healthcare information.* However, we have questions and concerns about this proposal that we would appreciate if CMS could clarify. First, it is unclear how this cumulative data would be accessed and seamlessly incorporated into a treating clinician's own EHR in a format that is useful for clinical decision-making, especially since CMS is not mandating that plans adopt a standard transmission solution (e.g. FHIR-based APIs). Second, as we noted earlier, health plans do not necessarily have access to all of the clinical data elements in the USCDI, which traditionally reside in a clinician's EHR. As such, how does CMS envision a health plan complying with this requirement if the payer does not have the full USCDI? It is absolutely critical that CMS impose restrictions on payers conditioning clinician participation in a plan based on whether a clinician will grant the payer electronic access to the practice's EHR to fulfill requests for the USCDI. We also have questions about liability if there is an error in the record. Under this proposal, if an error exists at any point in time, it could be replicated as the record accumulates. In this situation, who would be responsible for such errors or care decisions based on such errors? We request that CMS provide clarification on these critical issues. Finally, while this proposal has the potential to support more efficient and continuous care, such as preventing new prior authorization or step therapy requirements, it could significantly expand health plan access to a patient's clinical data, which could result in increased patient profiling to potentially limit coverage or access to care. We request that CMS provide additional details on what steps it plans to take to ensure that health plans do not use a patient's health information to increase prior authorization requirements or to otherwise limit access to care. Payers must be prohibited from using this information to discriminate against a beneficiary—both newly covered and those in the application process.

Care Coordination Through Trusted Exchange Networks

In this section of the rule, CMS proposes to require health plans to join a "trusted exchange network," which CMS believes would better facilitate the exchange of information between not only health plans, but also with providers and health systems. The trusted exchange network must be able to (1) exchange PHI in compliance with all applicable state and federal laws; (2) connect both inpatient EHRs and ambulatory EHRs; and (3) support secure messaging or electronic querying by and between patients, providers, and payers.

The Alliance appreciates that ONC recently updated its draft Trusted Exchange Framework and Common Agreement (TEFCA) to reflect public input and that it is once again seeking public input on these revisions.   In general, we support the concept of a trusted network that would better enable the secure flow of information from one entity to another. More specifically, we appreciate that the TEFCA aims to reduce the need for duplicative network connectivity interfaces, which are costly, complex to create and maintain, and an inefficient use of provider and health IT developer resources. As mentioned earlier, we also strongly support the fact that the Common Agreement would require non-HIPAA entities, who elect to participate in exchange, to be bound by certain provisions that align with safeguards of the HIPAA Rules since this addresses a critical ongoing gap in patient protections. *At the same time, we are*

concerned that plans may shift some of the costs of participating in these networks to patients and providers and request that both CMS and ONC remain mindful of that potential consequence.

Improving the Dual Eligible Experience by Increasing Frequency of Federal-State Data Exchanges

Currently, states can exchange beneficiary enrollment information with CMS as little as monthly. However, if Medicaid data is not updated with Medicare on a regular basis, coordination of benefits is delayed, which can result in inaccurate billings, confusion, and administrative hassles for both the patient and clinician, as well as wasted resources for states and CMS, which must reprocess claims. To minimize these inefficiencies, CMS proposes that states would be required to exchange certain Medicare/Medicaid data on dually eligible beneficiaries on a daily basis. *The Alliance supports requiring more frequent exchanges of this data as a way to eliminate current inefficiencies and improve benefit coordination for the dual-eligible population so long as this requirement does not impose additional reporting requirements on clinicians.*

Information Blocking

CMS proposes to publicly disclose when providers inappropriately restrict the flow of information to other health care providers and payers by including an indicator on Physician Compare for eligible clinicians/groups and hospitals who submit a "no" response to the prevention of information blocking attestations under the Promoting Interoperability (PI) Programs.   In the event that these statements are left blank, the attestations would be considered incomplete, and CMS would not include an indicator on Physician Compare. CMS would post this indicator on Physician Compare, either on the profile pages or the downloadable database, as feasible and appropriate, starting with the 2019 performance period data available for public reporting starting in late 2020.

The Alliance supports efforts to deter information blocking and shed light on truly "bad actors." However, we remind CMS that there are many specialists who are exempt from the PI category of the Merit-Based Incentive payment System (MIPS) because they are a Qualifying Advanced Alternative Payment Model Participant (QP), hospital or Ambulatory Surgical Center (ASC)-based, or qualify for a hardship exception (e.g. due to being a small practice or lacking control over the availability of Certified EHR Technology in their practice setting). We are reassured by CMS' proposal that in the event that these statements are left blank (i.e., a "yes" or a "no" response is not submitted), the attestations would be considered incomplete, and CMS would not include an indicator on Physician Compare. *We remind CMS to ensure that all clinicians who exempt from the PI category or otherwise not obligated to attest to the prevention of information blocking statements are not publicly portrayed as "bad actors" who inappropriately restrict the flow of health information. We also request that CMS consider including a disclaimer on Physician Compare explaining why some clinicians are not required to make these attestations.*

It is also important for CMS to keep in mind that the information blocking restrictions included in the 21st Century Cures Act, and promulgated through the ONC rule, will drastically change presumptions about data availability. As the Alliance explains in its comment letter to ONC, these new requirements are complex and ambiguous. When finalized, they are expected to leave clinicians confused about their obligations to, on one hand, share data in compliance with the new information blocking rules, but, on the other hand, to withhold data in order to comply with existing HIPAA requirements.   Confusion surrounding these two competing obligations may make it more difficult for clinicians under MIPS to affirm, with confidence, that they are not information blocking. *As we state in our comments to ONC, it*

is critical that all the relevant agencies within HHS work together to provide clear guidance to clinicians about their obligations under these evolving rules.

Provider Digital Contact Information

Under the 21st Century Cures Act, the Secretary is required to create a provider digital contact information index. CMS recently updated the existing <u>CMS National Plan and Provider Enumeration System (NPPES)</u>, which currently supplies and maintains NPI numbers, to be able to capture digital contact information (i.e., secure digital addresses) for both individuals and facilities. Health care providers are required to communicate to the NPPES any information that has changed within 30 days of the change. However, according to CMS, many providers have not yet added their digital contact information to NPPES and digital contact information is frequently out of date. To increase the number of providers with valid and current digital contact information available through NPPES, CMS proposes to publicly report the names and NPIs of those providers who do not have digital contact information in the NPPES system. CMS proposes to begin this public reporting in the second half of 2020, to allow individuals and facilities time to review their records in NPPES and update the system with appropriate digital contact information.

The Alliance supports the use of a provider directory to help providers find each other and to facilitate more efficient and secure sharing of health information between providers. This will not only help to enhance interoperability, but better support care coordination. At the same time, we have multiple concerns and questions about the details of this proposal. First, there is confusion among our member societies about what, exactly, CMS means by "digital contact information." On a recent call, CMS noted, "in regards to digital endpoint, an email address does not count. So, a provider should not be entering their Gmail or Yahoo or other private information, but it really should be their digital endpoint information which is certainly different and more secure." CMS also seemed to suggest that it would be a direct address that has been provided by the vendor, which could be used to exchange data from one EHR to another without having to use an external health information exchange resource. ***Since this terminology is vague and there is still confusion over this issue, we request that CMS clarify in the final rule what it means by "digital contact information" and provide more concrete examples and/or illustrations. We also request that CMS provide updated educational materials on the role of the NPPES and these new requirements, if finalized.***

It is also not clear where CMS would publicly post the names of providers who do not have digital contact information in the NPPES—would these names only be available to other providers or does CMS plan to share this information with the general public (e.g. through Physician Compare)? Furthermore, it is not clear how CMS would treat clinicians who do not have access to digital contact information (e.g., rural/small clinicians without EHRs or clinicians within larger systems who might not know their digital contact information or even know who to ask to get it). What protections would be in place to ensure they are not unfairly portrayed as non-compliant?

In light of all these unanswered questions and the many new responsibilities that providers may face as a result of both the CMS and ONC rules, the Alliance recommends that CMS use positive incentives, rather than public shaming or other disincentives, to promote accurate and up-to-date digital provider contact information in the NPPES.

Revisions to the Conditions of Participation (CoPs) for Hospitals and Critical Access Hospitals

CMS proposes to require, as a Medicare Condition of Participation (CoP), that hospitals electronically send "patient event notifications" to a patient's health care providers when a patient is admitted, discharged, or transferred. Notifications would have to include, at a minimum, the patient's name, the treating practitioner's name, the sending institution's name, and, if not prohibited by other applicable law, the patient's diagnosis). This requirement would be limited to only hospitals that possess EHRs with the technical capacity to generate information for these electronic notifications. Hospitals would only be expected to send such information to other providers that have an established care relationship with the patient relevant to his or her care and for whom the hospital has a reasonable certainty of receipt of notifications.

The Alliance supports this proposal in concept since it aims to improve transitions of care between medical settings and increase the safety, coordination, and quality of care overall. Nevertheless, we have heard from our members and colleagues that patient event notifications are already a widespread standard among hospitals. There is concern that this additional layer of regulation could disrupt clinical workflows and result in increased and unnecessary administrative burden for hospitals and hospital-based clinicians, who would be required to identify appropriate recipients of this information and to potentially determine whether or not a notification was successfully received by another provider. We are also concerned that if this requirement is formally tied to Medicare participation, hospitals will send more information than is required to ensure compliance, which could result in too much "noise" for the recipient provider and make it difficult to prioritize more critical patient information. *Since CMS seems to already have better mechanisms to ensure the exchange of appropriate health information for patients, we recommend that the agency instead focus on building the existing exchange infrastructure rather than layering additional requirements for hospitals to participate in Medicare.*

Advancing Interoperability in Innovative Models

In this section, CMS seeks input on ways to incorporate the promotion of interoperability into the design and testing of Innovation Center payment and delivery models. For example, CMS notes that new models could require that providers provide patients access to their own electronic health information and, upon the patient's authorization, to third party developers via APIs. *The Alliance supports the testing of innovative solutions to promoting interoperability so long as they account for provider costs associated with the implementation of these more standardized systems.*

RFI on Policies to Improve Patient Matching

CMS seeks input on how it could improve patient identification and linking patients to their health information to facilitate improved patient safety, enable better care coordination, and advance interoperability. While the federal government is prohibited from using funds to adopt a Unique Patient Identifier (UPI) standard, largely due to privacy and security concerns, it has the authority to evaluate alternative patient matching strategies that could evaluate and compare health information from multiple sources to identify common elements.

The Alliance agrees that patient matching is a critical issue. Although the process of linking the correct medical record to the correct patient seems like a basic task, it is one at which systems, even when made by the same EHR vendor, often fail. Inaccurate patient matching can lead to adverse events, compromised safety and privacy, inappropriate and unnecessary care, unnecessary burden on both

patients and providers, increased health care costs, and poor oversight of fraud and abuse. Furthermore, in the absence of mechanisms, such as a Unique Patient Identified (UPI), to ensure that relevant records are all tied to the same patient, safe and secure electronic exchange of health information is constrained. ***The Alliance appreciates that both CMS and ONC are looking into alternative solutions to this ongoing problem. While we do not have a specific recommendation, we urge both agencies to evaluate potential solutions, such as patient matching algorithms, carefully to ensure they do not exacerbate current challenges and lead to more errors or increased administrative burden.***

Conclusion

The Alliance supports CMS' goal of providing patients with easier and more complete access to their data so that they can become more engaged consumers of healthcare. However, it is critical that CMS not lose sight of the complexities and nuances of health care. Providing patients with unfettered access to data carries many potential unintended consequences that CMS and other federal agencies must carefully consider before our healthcare system can truly benefit from these proposals. While the proposals in this rule focus heavily on making it easier for patients to *access* their health care information, additional policies are needed to ensure that patients can actually *understand and meaningfully use* their health care information. In finalizing these proposals, we urge CMS to start small and proceed cautiously. The proposals in this rule represent a major paradigm shift with major implications, but they also hold great potential if implemented appropriately.

The Alliance looks forward to working with CMS to thoughtfully carry out these proposals. Should you have any questions, please contact us at info@specialtydocs.org.

Sincerely,

American Association of Neurological Surgeons
American College of Mohs Surgery
American College of Osteopathic Surgeons
American Gastroenterological Association
American Society of Cataract and Refractive Surgery
American Society for Dermatologic Surgery Association
American Society of Echocardiography
American Society of Plastic Surgeons
American Society of Retina Specialists
American Urological Association
Coalition of State Rheumatology Organizations
Congress of Neurological Surgeons
North American Spine Society
Society for Cardiovascular Angiography and Interventions