AMERICAN COLLEGE OF SURGEONS
Inspiring Quality:
Highest Standards, Better Outcomes
100+years

Chicago Headquarters
633 N. Saint Clair Street
Chicago, IL 60611-3211
Voice: 312-202-5000
Fax: 312-202-5001
E-mail: postmaster@facs.org

Washington Office
20 F Street, NW Suite 1000
Washington, DC 20001
Voice: 202-337-2701
Fax: 202-337-4271
E-mail: ahp@facs.org
facs.org

June 3, 2019

Ms. Seema Verma, MPH
Administrator
Centers for Medicare & Medicaid Services
Department of Health and Human Services
Attention: CMS-9115-P
P.O. Box 8011
Baltimore, MD 21244-1850

Re: 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 Ms. Verma:

The American College of Surgeons (ACS or College) is a scientific and educational association of surgeons, founded in 1913, to improve the quality of care for the surgical patient by setting high standards for surgical education and practice. On behalf of the over 80,000 members of the ACS, we appreciate the opportunity to submit comments to the Centers for Medicare & Medicaid Services (CMS) *Interoperability and Patient Access* proposed rule published on March 4, 2019 the *Federal Register*.

The ACS puts the welfare of our surgical patients above all else, and we support policies and regulations that promote high-quality care, reduce the regulatory burdens placed on physicians, streamline clinical workflow, and empower patients with data. As CMS engages in efforts to leverage health information technology (health IT) to support seamless and secure access, exchange, and use of electronic health information, access to patient data in this proposal presents very real challenges and unintended consequences which CMS must carefully address before this conceptual model can have a positive impact on patient care. The College, with its 100 year history in establishing standards for the national improvement of surgical care, stands ready to collaborate with CMS to work towards patient-centered interoperability. Improving access to patient data is critical, but what is even more important is ensuring that we are moving the right data, in the right way, and to the right person. In our letter, we highlight the following high-level comments that we believe will work to achieve the intent of 2st Century Cures:

- **Proposed interoperability conceptual model needs testing before large scale implementation.** While we support the conceptual model, the implementation is not ready without pilot testing due to the unlimited potential of unintended consequences. There are too many factors: too many middle-men, large data dumps without consideration for which information is appropriate for a given provider/phase of care. We need further clarification of the process and the expected role(s) of all stakeholders. For example, is it expected that the provider will act as an agent of the patient in gaining access to patient data?

- **We support a single standard for data exchange.** The adoption and enforcement of a single data exchange standard to accommodate plug and play sending of data with minimal burden on providers and patients is of critical importance for the success of these policies. Interoperability needs to happen across the entire care spectrum, and facilitated by a standard cloud platform, minimizing connections and individualized configuration. The standard should be used across all stakeholders: vendors, third-party developers, and payers.

- **There is a critical need for the certification of third-party application software and clinical logic.** As third party developers in the health space grow, ACS is worried about the efficacy of the clinical content and algorithms in new applications. As the Office of the National Coordinator for Health Information Technology (ONC) has not provided guidance on how and if this clinical data will be validated, verified, and certified, ACS is worried about the expectations of clinicians both on providing this guidance without reimbursement, and with sharing health data on their patients to an application without any form of clinical certification. As the Food and Drug Administration (FDA) has a certification and regulatory process in place for Mobile Applications, the ACS recommends that these criteria be adjusted and adopted in order to authenticate application developers.

- **Updated privacy and security standards for the digital landscape are needed.** As digital health continues to grow and expand, privacy and security standards need to be updated to keep pace with modern technology and the new and innovative ways in which patients and providers access and interact with health data. We request that CMS continue to work with other federal agencies such as ONC, the Office for Civil Rights (OCR) and the Office of the Inspector General (OIG) to more broadly re-evaluate current enforcement mechanisms in light of these changing dynamics and to expeditiously address these security and privacy gaps (i.e., beyond the Trusted Exchange in a way that is both binding and required). Current regulations should be updated to better ensure that data sharing will not occur unless a patient explicitly authorizes it and to limit the extent to which third-party/direct-to-consumer applications and other non–HIPAA-covered entities can use and share patient data.

- **Policies should enable the data flow of relevant and critical data, not all data.** The volume and type of data available to payers and patients should be appropriate and determined by an advisory panel. Patients receiving unnecessary or undefined data could result in an increase in providers' time to field questions, and payers receiving clinical data without context could result in the misuse of these data. It is vital that data sharing be done with specific, patient-centric, goals in mind: better care, better quality, and lower costs.

Our comments below are presented in the order in which they appear in the proposed rule.

<u>Technical Standards related to Interoperability</u>

In this section of the rule, CMS proposes to require Medicare Advantage (MA) organizations, state Medicaid and Children's Health Insurance Program (CHIP) fee-for-service (FFS) programs, Medicaid managed care plans, CHIP managed care entities, and Qualified Health Plan (QHP) issuers in Federally-Facilitated Exchanges (FFEs) to make patient claims and encounter data available to patients through an openly published Application Programming Interface (API). The APIs would, in turn, allow third-party applications ("apps") to make these data available to beneficiaries, with the approval and at the direction of the individual beneficiary, in a convenient and timely manner (e.g., through smart phones). CMS would require plans to offer open API access to beneficiaries for the following minimum set of data no later than one business day after a claim is processed or the data is received:

- Adjudicated claims (including cost);
- Encounters with capitated providers;
- Provider remittances;
- Enrollee cost-sharing; and
- Clinical data, including laboratory results, so long as it is managed by the plan;
- 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

CMS also proposes to require federal health plans to deploy API technologies conformant with the API technical standards proposed by ONC under the HIT Certification Program (i.e., HL7® FHIR®-based standards), which include security protocols such as authenticating end users' identities. However, CMS does not propose to require plans to use Health IT Modules certified under ONC's certification program. Furthermore, data elements would have to be formatted and presented in accordance with content and vocabulary standards known as the United States Core Data for Interoperability (USCDI v1). The USCDI v1 would replace the currently used Common Clinical Data Set (CCDS) and is expected to increase the baseline of data classes that must be commonly available for interoperable exchange. ONC expects that the USDCI will be updated annually to incorporate additional data classes and elements based on stakeholder input.

CMS proposes that APIs must be routinely tested to ensure they are functioning properly, including assessments to verify that the API is fully and successfully implementing privacy and security features such as, but not limited to, those minimally required to comply with the HIPAA privacy and security requirements and other applicable laws protecting privacy and security of individually identifiable health information.

These requirements would be effective January 1, 2020 (July 1, 2020 for Medicaid).

Overall, ACS supports CMS' goal of promoting the use of openly published APIs to enhance electronic health information exchange. An API is a set of software code and protocols that allow unrelated software programs to communicate with one another. They act as bridges between two applications, allowing data to flow regardless of how each application was originally programmed or designed, which is important in health care, as data sets can have different technical structures and the data terminology may not be consistent between HIT products, limiting interoperability. Because APIs are points of communications between systems, they can be used to simplify interoperability and provide clinicians, patients, and others with data more efficiently. APIs facilitate continuity of care by allowing health information to move through the health ecosystem with the patient, thereby ensuring comprehensive and timely information is accessible even if the patient changes health plans or providers.

In a more ideal world, EHRs would have open APIs. Also, any platform or cloud which separately holds a unified patient medical record from multiple EHRs and other data sources would also have open APIs. In this way, EHRs could provide data through FHIR®-based technical standards, to the patient unified record in the cloud and, in reverse, the unified patient record could use the same FHIR®-based technical standards to provide knowledge back to the EHRs. Such a set of open API processes would obviate the need for external sources to write into EHRs.

Technical Approach and Standards

We support CMS' decision to follow ONC's lead in taking the next step by requiring that APIs rely on FHIR®-based technical standards and USCDI-focused content and vocabulary standards. In regards to the FHIR®-based technical standards, although ONC had previously finalized an API functionality certification criterion in the 2015 Edition final rule (80 FR 62602), ONC has not required a specific standard for API functionality to date. The ongoing lack of such standards continues to make the exchange of data challenging and expensive since recipients often have to undertake substantial special effort to make sense of the information. In regards to the USCDI, we appreciate that this updated standard will improve the scale and scope of interoperability by including new data classes that are not currently captured through the CCDS. For example, the free text portion of clinical notes housed within electronic health records (EHRs) are a critical element of interoperable exchange, while the provenance of data (e.g., when and who created the data) is critical for improving the trustworthiness and reliability of exchanged data. We would strongly encourage CMS and ONC to continue to work with stakeholders to incorporate Digital Imaging and Communications in Medicine (DICOM) -based images into the USCDI. DICOM is a long-established standard that, among other things, supports the interoperable exchange of medical images. Currently, the USCDI v1 only includes the imaging narrative, but not the image itself. While the imaging report provides important information, surgeons need reliable access to the actual image to provide the most appropriate and cost-effective care.

We request that CMS provide additional details about how it envisions integrating administrative data made available by health plans with clinical data that may be housed in a clinician's EHR. Under the API proposal, plans would only be required to make clinical data available via API technology if they maintain such data as part of their normal operations. However, plans typically do not manage such data (e.g. clinical notes, imaging results, and lab results). We ask for clarification on exactly what plans are being asked to share that they do manage—is CMS asking plans to share billing codes for medical tests, information on in-network providers, patient demographic data, or something else? **Given the importance of clinical data for medical decision-making, we request that CMS clarify how it plans to ensure that patients and their clinicians have access to more than simply administrative plan data.**

In general, the ACS appreciates the value of empowering patients with data. With easier, more comprehensive access to health records and related information, patients can better understand, advocate for, and manage their own health care. Having this access also enables patients to more easily share this information with providers, family, and caregivers, thereby supporting greater care coordination. At the same time, it presents very real challenges and potential unintended consequences that CMS must carefully address before this initiative can have a positive impact on patient care. For example, while **there is no doubt that the FHIR® and USCDI standards, proposed by both CMS and ONC, will move the needle in regards to interoperability, these standards, alone, are insufficient. These standards will advance *technical* interoperability in that they will improve the ability to transmit data from one place to another. However, they will not necessarily achieve *semantic* interoperability, or the ability to transmit data from one place to another with meaning**.

As noted in a 2018 Medical Economics article[1], "The FHIR standard will be challenged in the realm of semantic interoperability because of the use of different coding systems which will require data normalization regardless of the transport technology employed. As a simple example,

[1] D'Amore, J. Interoperability: The FHIR standard is not a panacea. Medical Economics. Nov. 2018. Accessed at: https://www.medicaleconomics.com/technology/interoperability-fhir-standard-not-panacea

Source A may provide an ICD-10 code for Heart Failure while Receiver A is expecting a SNOMED code. Mapping the ICD-10 code system to SNOMED would be required for semantic interoperability. While this is a simple example, clinical data created by hundreds of certified HER documented by millions of clinicians are highly de-normalized and require technology middleware for effective, scalable data normalization." As noted in that same article, health IT developers are creating "read only" FHIR resources and not supporting the capability to write back to the EHR, which limits use cases. To achieve true and more widespread interoperability, ONC and CMS must work together to ensure that both the interface technology and underlying data are standardized and transparent and that all systems are speaking the same language. The agencies also need to collaborate to ensure that software receiving the data can readily process it and translate it as necessary, and then build out user-friendly displays and other functionalities.

To allow for the desired interoperability described above, ACS encourages CMS to work with ONC to ensure EHR certification standards are compliant with open source digital standards that meet criteria for clinical interoperability. This would greatly aid in data liquidity, which would largely eliminate data blocking, and enable patient cloud environments. The cloud environments could provide data processing and transformation through algorithms, allowing EHRs to connect to a platform built on a reference standard and a reference architecture upon which a vendor can assemble a FHIR-based unified patient record instead of multiple, proprietary interfaces. This standardized platform can provide an open API to a variety of third party applications, health information exchanges (HIEs), registries, and other EHRs, achieving data normalization. Further, updated standards and a shared cloud platform would allow EHRs to query and pull down needed data, creating the opportunity to directly incorporate external data after clinical reconciliation has been performed, and creating a complete health record for the patient within a provider's EHR. Promoting data be sent and received in a single, standard format will better enable this bidirectional exchange, particularly when facilitated through a single cloud platform.

The ACS is also concerned that this proposal has the potential to overwhelm and confuse patients and their caregivers, who will be granted access to an unprecedented amount of information that will be difficult to interpret and prioritize, particularly administrative claims data from payers that may not be relevant to care management. Similarly, this proposal has the potential to overload providers with extraneous information, as well as new responsibilities related to communications with patients and caregivers who will increasingly turn to providers for clarity regarding things like concerning test or lab results not directly related to the care for a specific provider. With information at their fingertips, patient expectations will also rise in terms of provider accessibility and response times. We are already seeing that as API use becomes more widespread, data (e.g., lab results) increasingly reaches the patient before it reaches the clinician, which often leaves the clinician unprepared to respond to the patient in a meaningful manner. With the rise of patient portals throughout the Meaningful Use Program, providers and their care teams were often overwhelmed by questions from patients as they received lab and test results through their patient portal before providers or their care teams were able to review them. Even with guidelines for interpreting and understanding the results, patients often preferred to discuss the results with their provider. ACS is concerned that this volume of patient inquiry will increase as there are new sources of clinical data available to the patient in real-time, with no plans for adjusting reimbursement methodology. Translating data into consumable knowledge for patients through proper communication and education filters will take time to develop. ACS has concerns that these additional burdens are not recognized by the current resource needs in a typical surgical practice.

Patients and caregivers are also expected to turn first to their providers when they receive confusing health plan claims and cost-sharing information, putting pressure on providers to explain payment decisions that they likely have no control over. We also expect that providers will be called upon to provide clinical expertise to third-party app developers as they attempt to present data to patients in simple and accurate formats. The ACS recommends that CMS and ONC work together to develop a standard to use for third party application certification. As the FDA has a certification and regulatory process in place for Mobile Applications, the ACS recommends that these criteria be adjusted and adopted in order to authenticate application developers. Additionally, just as critical is the 1) certification of the clinical logic used to ensure that the products are safe, accurate, and in alignment with clinical guidelines, and 2) privacy certification to ensure that apps meet privacy standards. We encourage leveraging the expertise of professional society organizations to certify the clinical logic. In the current marketplace, it is our understanding that HIT developers employ hold-harmless clauses that protect them from liability if hospitals are later sued for medical errors that resulted from defects in the software. We believe that third-party app developers should be held responsible for medical errors—certification of technology and clinical logic would largely eliminate this concern for users and developers of apps. Many providers already feel that their clinical time has been significantly eroded by a variety of administrative and EHR-related disruptions, and these new demands and expectations will further shift this imbalance.

Privacy and Security Concerns in the Context of APIs

ACS also has concerns about the manner in which patient data access could alter the medical liability landscape. As providers gain access to more longitudinal patient records and external data, it is not reasonable to expect them to review and take responsibility for the entire universe of data that is accessible to them. For example, a cardiologist should only be expected to review information relevant to the field of cardiology and to the patient's specific condition. If the patient's record includes a radiology report that indicates a tumor growth in a scan of the abdomen, it would be unreasonable to expect the cardiologist to have opened or reviewed that file. As patient records are aggregated over time, there is also an increased risk for errors being duplicated over time. We request that CMS clarify who would be responsible for such errors. For instance, if an inaccurate diagnosis was entered in an external provider's system and was transferred into the patient's health record, as interoperability becomes easier, this inaccurate diagnosis could be incorporated not only into the patient's EHR, but also in HIEs, third-party apps, and in claims data. Having provenance data attached to or incorporated with shared data, as proposed in the ONC rule, would identify the original source of data. It should be the original source of the information where liability lies if and when errors occur. We request that CMS clarify that this is the case. To avoid such errors, the patient and their provider(s) can work together to ensure the data included in their complete health record is clinically accurate, particularly as external sources are available and integrated. However, as this is another burden on providers, this also needs to be taken into consideration by CMS when determining and setting payment policies. Additionally, if patients are able to alter or add data and information to their health record, either through their patient portal or another mobile health application, ACS is concerned about what is viewed as the source of truth. Does the EHR remain the legal medical record, and does it remain at the provider's discretion to accept or integrate external data, even if it comes from the patient? ACS requests clarity and guidance on these topics.

Finally, the ACS is concerned about the privacy, security, and general use of data once it gets into the hands of third-party entities, which are often considered "non-covered entities" under HIPAA. These include companies that develop fitness trackers or other mobile software and cloud-based tools that collect, store, and share personal health data, but also social media services that are set up to allow individuals to share health information or experiences. **The proposals in the CMS and ONC rule will drastically increase the number of these entities and places where patient health data is collected, stored, and transmitted, as well as the format and tools through which the data is entered and viewed, yet many of those organizations will not be subject to the same rules concerning the protection of Protected Health Information (PHI) as traditional healthcare organizations.** We ask CMS to clarify what protections are in place to stop these entities from using, selling, or otherwise sharing personal health information without the patient's permission. Even with permission, there is a real risk that direct-to-consumer applications could disclose an individual's confidential information in a manner that is inconsistent with the privacy notice and terms of use to which the individual agreed and understood.

Perhaps most concerning is that these proposals will inevitably turn patient data into a commodity, which will put it at increased risk for misuse and other abuses that could impact security and privacy, coverage, access to care, and further interfere with the physician-patient relationship. For example, third-party developers of health apps may have no experience with clinical medicine or performance measurement, yet they could easily use aggregate patient data to make unqualified judgements about providers. In a free market, patients and clinicians also need assurances that third-party apps are vetted for data security. We recommend that ONC work with stakeholders to develop a certification process— for both APIs and the applications that communicate with them— that would require developers to demonstrate the testing of their products, to attest to taking appropriate measures to protect the safety and privacy of data, and to verify the appropriateness of the clinical algorithms embedded within the technology.

As the FDA has a certification and regulatory process in place for Mobile Applications, the ACS recommends that these criteria be adjusted and adopted in order to authenticate applications. Additionally, just as critical is the 1) certification of the clinical logic used to ensure that the products are safe, accurate, and in alignment with clinical guidelines, and 2) privacy certification to ensure that apps meet privacy standards. We encourage ONC to leverage the expertise of professional society organizations to certify the clinical logic.

In the case that standards from the FDA's existing certification process are not developed and utilized, ACS suggests using the below three "yes/no" adoption & implementation attestations as a part of the certification requirements in order to ensure adherence to privacy standards:

(1) *Industry-recognized development guidance* (e.g., Xcertia's Privacy Guidelines);
(2) *transparency statements and best practices* (e.g., Mobile Health App Developers: Federal Trade Commission (FTC) Best Practices and CARIN Alliance Code of Conduct); and
(3) *a model notice to patients* (e.g., ONC's Model Privacy Notice).

The certified app could then be acknowledged or listed by the health IT developer (e.g., in an "app store," "verified app" list). EHR vendors could also publicize app developers' attestations.

Without the certification of the technology and clinical logic, the responsibility of verifying the authenticity of mobile applications could fall on the shoulders of patients and providers who do not have the resources, time, or expertise to conduct such assessments. Further, in the event that the apps are not certified by any process, ACS seconds the ONC's statement that these apps would not have carte blanche access to a health care provider's data. Such apps would still be registered and thus identifiable and able to have their access deactivated if they behave in anomalous or malicious ways. Furthermore, we support the fact that a patient seeking access to their data using the app will need to authenticate themselves (using previously issued credentials by a health care provider or trusted source) and authorize: 1) the app to connect to the FHIR server; and 2) specify the scope of the data the app may access. Overall, the ACS objects to policies that place a disproportionate burden on physicians in terms of resources and time and that lack privacy and security standards, as well as clinical and technical logic certifications.

In a 2016 ONC report titled, Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA,[2] the ONC explains that privacy and security protections for health information have not kept up with technology and 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." The ONC also expresses concern that data security and privacy protections may not be sufficiently robust to prevent accidental disclosure or theft of

[2] The Office of the National Coordinator for Health IT. Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA. June 2016. Accessed at: https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf

data, yet many consumers may mistakenly believe that their data – and their privacy – is protected and covered by federal laws. The ONC does not recommend broadening the definition of “covered entities,” but says there are serious security gaps at non-HIPAA covered entities and that those gaps must be addressed. More recently, the ONC released the second draft of its Trusted Exchange Framework and Common Agreement (TEFCA), clarifying that non-HIPAA entities who elect to participate in an exchange would be bound by certain provisions that align with safeguards of the HIPAA Rules. We agree with ONC that these expanded protections will bolster data integrity, confidentiality, and security, which is necessary given the evolving cybersecurity threat landscape. **We request that CMS continue to work with other federal agencies such as ONC, the OCR and the OIG to more broadly re-evaluate current enforcement mechanisms in light of these changing dynamics and to expeditiously address these security and privacy gaps (i.e., beyond the Trusted Exchange in a way that is both binding and required). Current regulations should be updated to better ensure that data sharing will not occur unless a patient explicitly authorizes it and to limit the extent to which third-party/direct-to-consumer applications and other non–HIPAA-covered entities can use and share patient data.** Guidance may also be needed to clarify potential misuses of data. Without consistent standards for the protection of health information for non-covered entities, patients will continue to face a high risk of having their health data exposed, stolen, or misused.

Regardless of what action regulatory action is taken, federal agencies need to work more immediately to educate patients about the implications of sharing their data with third-party entities that are not non-HIPAA-covered entities and the potential for data to be potentially commoditized or otherwise misapplied. Consumers may lack an understanding of the entities that are required to comply with HIPAA and those that are not. For example, they may not understand that HIPAA does not apply to fitness trackers or other commonly used portable devices or apps that are used for medical purposes. They also may not have a good understanding of how the new requirements proposed in this rule permit other parties to obtain and use their data, which will create the potential for further vulnerabilities. We appreciate that CMS proposes specific requirements for payers to ensure enrollees understand how to protect their PHI, important things to consider when selecting a third-party application, and where they can file a complaint if they believe that 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 and how their information could be used. It is equally important for these federal agencies to educate the provider community about these new risks, as well as what role and obligations the provider has in terms of making data available, authenticating the identity of requestors of data, and otherwise authorizing access to data.

Patient Access Through APIs

Expanding the Availability of Health Information

CMS proposes utilizing API technology to enable plans to share claims and encounter data directly with enrollees and beneficiaries. Through the use of the API standard, plan data could be available to enrollees through third-party applications, providing a streamlined way to request, receive, and share information. CMS envisions that this type of access will not only enable enrollees to better understand their health and care options, but will also allow patients the option through standard technology to share plan data with providers, creating a more complete record.

The ACS is concerned that CMS' API proposal is specifically aimed at ensuring health plans provide data access to *enrollees*. CMS simply encourages payers to *consider* using the proposed API infrastructure as a means to exchange PHI for other health care purposes, such as to health care providers for treatment purposes, or suggests that enrollees could share these data with their providers. However, there is no specific obligation for plans to share these data with providers at this time. As CMS recognizes, effective care coordination between plans and providers can inform health care providers about where their patients are receiving care to better understand the totality of their healthcare needs and manage their care. Sharing plan data with a provider's EHR ahead of time could save time during appointments, reduce duplication of services, and ultimately decrease costs and improve the quality of care delivered to patients. It would allow providers to more easily integrate claims and encounter information with clinical data stored in the EHR and to integrate that combined data into relevant clinical decision support and patient education tools. We request that CMS accelerate efforts to support the sharing of data between health plans and providers, as well as require plans to receive consent from enrollees before sharing their data, even when aggregated. Further, we ask CMS to consider a requirement for payers to provide data to providers, in the same format and standard as provided to enrollees.

Open API Proposal for MA, Medicaid, CHIP, and QHP issuers in FFEs

Provider Directory Data

Provider directory data are one of the types of data that CMS proposes to make available through open access APIs. CMS proposes to specify that MA Organizations (MAOs) make specific provider directory information for their network of contracted providers accessible through their APIs including the names of providers, addresses, phone numbers, and specialty. MAOs would be required to ensure the availability of this information through their APIs for all MA plans. MA 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. These data, including updates to such data, would be available to not only their enrolled beneficiaries and patients, but also to the public at large for purposes of prospective enrollees reviewing whether a provider is in network, as well as for the purposes of referrals. Clinicians could use these APIs to locate an in-network provider for one of their patients before sending them off for a referral or for other purposes for which care coordination is needed.

Currently, CMS requires MAOs to post on their websites their network of contracted providers (including the names, addresses, phone numbers, and specialties of such providers). MAOs must maintain accurate online provider directories that list only actively contracted providers with specific notations for those who are not accepting new patients. In the event that a change is made to an MAO’s network, the organization must make a good faith effort to provide written notice of a termination of a contracted provider at least 30 days before the termination effective date to all enrollees who are patients seen on a regular basis by that provider; when a contract termination involves a primary care physician (PCP), all enrollees who are patients of that provider must be notified.

The ACS strongly supports easy access to up-to-date and correct provider directory information. Making provider directory data available through open APIs will improve the ability of MAOs to comply with the requirement to update this information. Accurate provider directory data will also improve transparency and accessibility of information regarding a provider’s network status, which will help with efforts to address surprise billing and other coverage issues related to whether providers are in or out-of-network. In order to make locating relevant information as easy as possible, patients, providers, and others should have the ability to make focused requests for specific data in order to avoid receiving a data dump of provider information.

We also stress the importance of a centralized repository for provider data. This is a key component missing from the accurate provider directory equation, and we support CMS' ongoing efforts at looking at the provider data collected by MAOs to determine how it may be used to foster a collaborative industry approach to achieving a central location for such data. Currently there is no centralized repository for provider directory data, and the current process of verifying the accuracy of provider information can present an undue burden on providers since they must complete the same set of validation questions for each of the multiple MA plans they may contract with. A centralized database could allow the current inward facing MAO efforts to have a broader impact. For example, when an MAO identifies a directory error, it currently is fixed only for their own directory, whereas a corrected error in a centralized database would improve directory accuracy for all MAOs using that system. Enabling provider directory information to be shared via open APIs could aid in this effort toward a centralized provider directory as well.

Timeline

Regarding the timeline, CMS states that plans must make data available through an API no later than one business day after a claim is adjudicated or the encounter data is received by the plan. While we support the stipulation "after a claim is adjudicated," we are concerned this proposal will put unnecessary pressure on network clinicians to submit a bill immediately after a day of service. We support timely access to data, but request that CMS reconsider the "one-day" requirement as plans and clinicians adjust to new API and other data access policies, and recommend three business days as a reasonable alternative. The ACS asks for clarity on how CMS plans on enforcing this, as well as what the consequences will be for not meeting these requirements.

Monitoring and Testing

ACS also supports CMS' proposal that payers must conduct routine testing and monitoring of APIs to ensure they function properly and have appropriate privacy and security features. However, we are confused about the plan's actual role in this process. Where would a plan house its API technology? Is it the plan's or the API developer's responsibility to test and monitor it? We would greatly clarification of these details, including a visual depiction in the final rule. We are also concerned that adherence to these requirements (by either the payer or the EHR) will require investments that may be passed on to providers. While plan enrollees seem to be protected from these costs, providers are not.

In light of the numerous concerns identified in this section, as well as CMS' acknowledgement that substantial work still needs to be done by health IT developers and their customers to build and deploy technology to support these proposals, we also ask CMS to reconsider the January 1, 2020 implementation. 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, and we recommend extending the timeline to a January 1, 2021 implementation.

In conclusion, the ACS strongly urges CMS to carefully consider all of the potential implications of making data more accessible through the use of APIs, and to address these concerns in the final rule.

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 such a process could leverage the APIs proposed in this rule. ACS recommends that providers are given access to patient specific payer data via API technology, similarly to the proposal for payers making data available to enrollees. However, the payer data must follow standards, such as USCDI, and follow a specific clinical logic for a given domain to ensure that providers only receive information that is relevant to clinical care. This is a very complex mapping process and should be done in partnership with professional society organizations. The ACS is currently using grouper logic to define services across the various phases of surgical care in order to determine if certain services are necessary or unnecessary, and is familiar with this process. To be sure the data are shared in a comprehensive and logical way, and that data do not instead present administrative burdens to the provider, pilot testing needs to be conducted before any requirements are put into place.

Health Information Exchange and Care Coordination Across Payers

CMS also proposes to require certain health plans to exchange a minimum set of data (i.e., the USCDI v1 data set) upon an enrollee's request. Plans would be required to:

- Accept the data set from another plan that had covered the enrollee within the previous 5 years;

- Send the data set at any time during an enrollee's enrollment and up to 5 years later, to another plan that currently covers the enrollee; and
- Send the data set at any time during enrollment or up to 5 years after enrollment has ended to a recipient identified by the enrollee.

The ACS supports policies that aim to enhance communications between payers and believe this proposal could help the payer and the patient reach optimal care, reduce duplication, and decrease costs long term. If also shared with clinicians, this longitudinal record of a patient's medical care could reduce unnecessary screenings and assessments, reduce repeated utilization reviews, streamline prior authorization processes, and reduce instances where a clinician needs to intervene personally with the enrollee's plan to ensure his or her patient receives the necessary treatment.

However, we are concerned about potential unintended consequences that could result from these new requirements. This proposal, if finalized, will result in large, unprecedented data streams for which with no way to guarantee validity and reliability. There are multiple potential implications of expanding access to this compiled information, including liability concerns, which CMS needs to carefully consider before finalizing these policies. For example, as we noted earlier, as patient information is shared and a more longitudinal record compiled over time, there is a substantial risk of errors due to both human error and differences in each systems' mechanisms for information protection, sharing, storage, and classification. If an error is made in one place, that error will then be replicated, making the importance of recording accurate information even more critical. We would appreciate if CMS could further elaborate on the responsibilities and potential liabilities of a provider who encounters erroneous information within a patient record or who makes a medical decision based on that erroneous external data.

Furthermore, expanded access to data raises concerns about potential liability in regards to resource use. As clinicians have expanded access to a more comprehensive and longitudinal patient record, they may determine that care provided by a previous clinician was inappropriate or insufficient and may feel the need to re-order tests to ensure accurate diagnoses. In such cases, could a clinician be penalized for what might appear as over-utilization of services? As CMS widens access to patient data, it is critical that it consider new protections, and at the very least develop clear guidance, so that providers understand their responsibilities when navigating these expanded troves of data. It is equally critical that

CMS adopt policies to preserve and protect clinician autonomy in care decisions.

Under this proposal, CMS also would permit plans' flexibility in terms of electronic exchange methods by not requiring them to use a standardized format for data exchange (e.g. FHIR-based API). The ACS does not support this proposal and urges CMS to require that plans adhere to FHIR standards for exchanging data. By not adopting a standard for exchange, CMS will be making it more challenging for plans to combine data, which could result in confusing formats for patients/providers, inconsistent formats. As the ONC is proposing to require FHIR-based API, CMS should require the same standard for consistency and to ensure the ability to share data between payers and providers is based on the same standard of exchange. In addition to adopting a standard for health plan exchange of data, we would support CMS requiring these plans to create provider dashboards that make it easy for providers to access all information about their patients. Furthermore, we also request that CMS provide additional clarification on how this proposal would support patients and providers in situations where a plan subject to this requirement may be exchanging patient health information with another plan that is not similarly required to exchange USCDI data sets for enrollees.

Finally, our comments in this section assume that patients are sharing this longitudinal data with providers, but nothing in this rule actually requires that they do so. We again request that CMS develop policies that would ensure that clinicians making medical decisions at the point of care have seamless access to patient data from all external sources.

Provider Digital Contact Information

The Secretary required that CMS create a provider digital contact information index under section 4003 of the Cures Act. This index must include all individual health care providers and health care facilities, or practices, in order to facilitate a comprehensive and open exchange of patient health information. CMS has chosen to update the CMS National Plan and Provider Enumeration System (NPPES) to be able to capture digital contact information for both individuals and facilities. NPPES currently supplies NPI numbers to providers (both individuals and facilities), maintains their NPI record, and publishes the records online. Health care providers are required to communicate to the NPPES any information that has changed within 30 days of the change. NPPES has been updated to include the capability to capture one or more pieces of digital contact information that can be used to facilitate secure sharing of health information; however, many providers have not yet added their digital contact information to NPPES and digital contact information is frequently out of date. CMS doesn't explicitly define "digital contact info" but provides the following examples of electronic addresses: Direct address, FHIR server URL, query endpoint, or other digital contact information.

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 included 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 ACS believes that a regularly updated provider digital contact information index is important for supporting enhanced interoperability. However, we request that CMS provide clearer guidance on what it means by "digital contact information" and how it would treat the following:

- 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)
- Clinicians that work within multiple EHRs (which digital address would they provide and if they would be expected to provide all of them, how would users of the system know which one to use for communications with that clinician?)

<u>Revisions to the Conditions of Participation (CoPs) for Hospitals and Critical Access Hospitals</u>

In this section, CMS proposes to require as a condition of Medicare participation that hospitals electronically send "patient event notifications" to a patient's health care providers when a patient is admitted, discharged, or transferred (ADT). The requirement would be limited to only hospitals that possess EHRs systems with the technical capacity to generate information for these electronic notifications. These 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. Hospitals must utilize specific content exchange standards and notifications must include the minimum patient health information, which is patient name, treating practitioner name, sending institution name, and, if not prohibited by other applicable law, patient diagnosis. CMS recognizes that many existing ADT messaging systems might not include diagnosis and seeks comment on the technical feasibility of including this information.

While the ACS supports this proposal in concept, we are concerned that by relying on the CoP process, this proposal could add another unnecessary layer of regulation to a practice that is already relatively common in hospitals. If over-regulated, hospitals may send more information than is needed to community providers out of a fear of non-compliance. This could result in signal fatigue for recipients of these notices and require them to sift through a large amount of potentially irrelevant information simply to find what is most important for the patient under their care.

We are also concerned that it would be time-consuming and potentially challenging for hospitals and the clinicians practicing in those hospitals to determine other relevant provider recipients and whether those recipients have the capacity to receive such information. We request that CMS clarify what criteria hospitals would be expected to use when determining recipients and reasonable certainty of receipt of notifications. For example, must the hospital attempt to send the notification and document a bounce back to demonstrate that the message did not go through? As currently written, these proposals are vague and could result in significant documentation burden for hospitals and surgeons who practice in them. Additionally, ACS asks for clarity on if this will remain a requirement for providers and health systems already utilizing an HIE, as this information would be available through the HIE. Some HIE systems also provide push notifications to providers when any of their assigned patients are admitted to the hospital or have an emergency room visit. This proposal would duplicate this existing set-up, and create additional administrative burden for providers.

CMS intends for these notifications to be required, at a minimum, for inpatients admitted to, and discharged and/or transferred from the hospital. However, the Agency seeks comment on whether it should identify a broader set of patients to whom this requirement would apply, and if so, what those parameters are. The ACS believes this policy should apply to all urgent and emergent care, as well as patients in observation status who have not yet been admitted to the hospital, but are under the hospital's care. Furthermore, while this proposal would require hospitals to send a notification to a community provider that a patient was admitted to the hospital, it is equally important that a community provider share information about the patient with the hospital upon receiving a notification that the patient was admitted. For example, congestive heart failure (CHF) is a big predictor of post-operative complications. It is critical that a surgeon treating a patient recently admitted to the hospital is aware of the patient's comorbidities. However, it is also critical that providers only send and receive information relevant to the care they provide the patient so as to not overburden providers with unrelated patient information. CMS should work with stakeholders to develop a clinical logic that can be applied to this process.

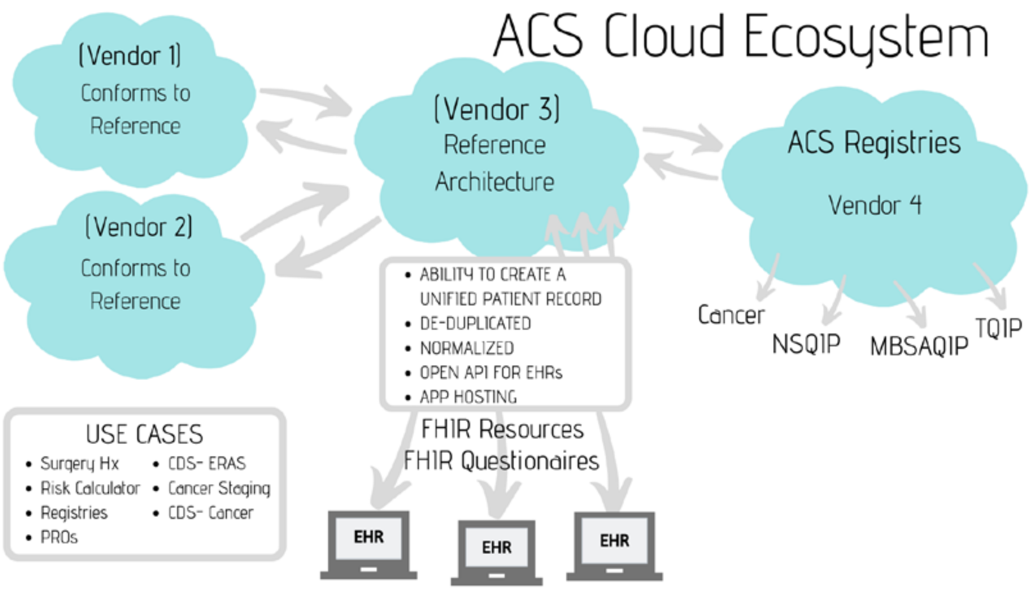
CMS proposes that hospitals must use the HL7 ADT Messaging standard Version 2.5.1. Recognizing that there is significant variation in how hospitals have utilized the ADT messages to support implementation of patient event notifications, CMS proposes to require that hospitals possess a system utilizing this standard, but they may utilize other standards or features to support their notification systems. CMS' intent is to set a baseline for hospitals' capacity to generate information for electronic notifications, while still allowing for innovative approaches that could increase the effectiveness of these notifications in the future. The ACS questions whether the operational systems are readily available to transmit and accept these data without disruption to clinical workflows. We also advise against policies that would allow hospitals to deviate from required standards since a lack of consistency could pose a barrier to effective implementation. We also urge CMS to consider mirroring the same standards the ONC is proposing for interoperability to ensure consistency across all types of data exchange. Finally, if CMS is to finalize this proposal, we agree that notifications must, at a minimum and if not prohibited by other applicable law, include patient diagnosis. Diagnosis is one of the most important pieces of information for the surgeon, and we urge CMS to preserve this as a requirement.

RFI: Advancing Interoperability across the Care Continuum

CMS recognizes that transitions of care have long been a sticking point for data sharing and interoperability, particularly for patients with complex treatment needs. For long term care, behavioral health, and home and community based services, the challenges have been greater due to a lack of uniformity in the adoption of HIT systems. The challenges in data sharing have contributed to increased hospital readmissions, emergency department visits, and other adverse outcomes. ACS agrees that this has been a challenge across the entire care continuum, and supports standards that will increase the ease and feasibility of sharing clinical data across transitions, including long term care and behavioral health care.

Advancing the surgical care continuum involves patients who are coming to the surgeon from outside the system, and who may also continue their care in another external system. To fully take care of patients with the highest quality, it is vital for surgeons to have access to their health data from all prior providers and points of care. As such, data exchange from their Primary Care Provider, as well as from any past surgical events, emergency visits, and hospital admissions, is necessary in order to provide the best surgical care. A full patient history, including diagnoses, medications, allergies, imaging, and notes better allow surgeons to have the complete picture and all of the necessary data points to make the best and most appropriate care choices for their patients. Further, when the patient leaves the Ambulatory Surgery Center or the hospital to receive post-surgical care, either through outpatient care or through a post-acute care facility, this complete medical record should follow them through their care journey. This will also facilitate better care management, and streamline the touchpoints throughout the system to the patient.

In order for data to follow the patient with minimum burden on the provider to exchange and view—and integrate, when appropriate—the standards for interoperability must be consistent and required. Creating innovative standards and solutions for interoperability begins with patent-centric solutions, such as a cloud platform that acts as the pass through for data from a variety of systems, including EHRs from all vendors and mobile apps, and acts as a processing system to translate data when needed into the correct format and standard to then share back to external systems (an EHR on another instance, a clinical data registry, a research database, etc.). As illustrated in the following figure, data would be sent to the cloud platform via APIs that rely on FHIR®-based technical standards, as certified-EHRs and mobile technology will be using these standards as a result of the ONC interoperability regulations. As all systems develop using the same standards, it would also create the possibility for the bi-directional flow of data available through an open API, providing the opportunity for providers to pull down and incorporate data back into their EHRs when it is appropriate and relevant for the course of patient care. This complete patient record, when also including data from payers, external providers, and community-based care systems, will not only provide higher quality care as providers have all of the needed clinical data in a single system, but it also has the capacity to decrease duplicative care, target preventative care at the right time, decrease administrative burden on providers and care teams, reduce fraud, and provide patients with better tools and information for their own care management.



PROs: Patient Reported Outcomes
CDS: Clinical Decision Support
ERAS: Enhanced Recovery After Surgery
Improvement Program

TQIP: Trauma Quality Improvement Program
NSQIP: ACS National Surgical Quality
MBSAQIP: Metabolic & Bariatric Surgery
Accreditation and Quality Improvement Program

Advancing Interoperability in Innovative Models

Using authority under the Center for Medicare and Medicaid Innovation ("Innovation Center"), CMS plans to test innovative solutions to further promote interoperability. Through both payment and service delivery models, CMS asks for new models for data sharing that incentivize high quality and efficient care while reducing program expenditures. ACS appreciates that CMS is continuing to look for innovative solutions to ease burdens of data sharing across the care continuum and across digital tools.

ACS sees real opportunities for innovation within surgical care models using episodes of care to measure value and create innovative reimbursement methodologies. Vital to this value-based care framework is the ability to leverage both quality data and cost data across the patient's care journey. The value expressed for a condition or a procedure can be used by patients to select their provider or by a payer for inclusion in a value-based incentive. Furthermore, the value expressed can be used in physician compensation models to push value directly rather than volume. Also important is that the appropriate timeframe for assessing the quality and cost fits the condition. As an example, a prominent cancer hospital was examined for the annual cost of care provided for breast cancer treatment and was found to be one of the most expensive centers nationally. But when the cost data was analyzed longitudinally for 10 years, as opposed to 1 year, the center was found to have much lower costs than other centers due to the high quality of care provided and low recurrence rates. Although in the first instance the value appeared to be low due to high cost, when taking a longer view of the time period, the center was found to provide extremely high value care. Therefore, one aspect of assessing quality involves considering the appropriate time window for a true picture of the value. CMS should consider the timeframe and types of data sources included for determining reimbursement methodologies, and ensure that data sharing incorporates all the necessary elements to provide a complete picture of quality, value, and cost across the care continuum. Interoperability should not be the end goal; rather, the seamless exchange of meaningful data for a variety of purposes, including improving quality and managing cost, should be the long-term vision of these innovative models.

RFI on Policies to Improve Patient Matching

CMS notes that there has been considerable feedback about the challenges of patient matching across platforms, systems, and data types without a unique identifier for each patient. Without such an identifier, safety and privacy concerns are heightened and interoperability challenges increase, as there is no failsafe methodology for ensuring that the relevant records being exchanged are for the same, and for the correct, patient. However, as HHS was prohibited from using funds to adopt a UPI standard, largely due to privacy and security concerns, there is a critical need to develop patient matching strategies that would evaluate and compare health information from multiple sources to identify common elements and mitigate risk.

ACS agrees with the feedback that CMS has received that the lack of a Unique Patient Identifier (UPI) inhibits interoperability efforts and introduces patient safety risks. Inaccurate patient matching can lead to adverse events, compromised safety and privacy, inappropriate and unnecessary care, unnecessary burden on both patients and providers to correct misidentification, time consuming and expensive burden on health systems to detect and reconcile duplicate patient records and improper record merges, increased health care costs, and poor oversight of fraud and abuse. Inaccurate data matching poses a significant risk to patient safety because information may be unavailable when needed or records may be merged incorrectly, leading to inappropriate treatment choices. Errors in individual data matching will be compounded with the expansion of electronic health information sharing, as proposed in this rule.

In the absence of a legislative fix mandating the creation of a UPI for this issue, the ACS recommends that CMS and ONC continue to explore alternative solutions for this problem. A standard algorithm hosted in a cloud platform that assesses and determines patient matches based on identifying information, such as name, date of birth, Payer ID, or other unique identifiers could be a stop-gap solution. Further, standard requirements for patient identifiers as part of the USCDI, such as number of digits and inclusion of hyphens, dashes, and apostrophes, could aid in this issue by standardizing the name field in EHRs and third-party applications. However, these options will not solve this problem completely, and ACS encourages a larger legislative fix for this issue, as it will only grow in size as digital technology continues to increase in scope and practice.

The ACS appreciates the opportunity to provide feedback on this proposed rule and looks forward to continuing dialogue with CMS on these important issues. If you have any questions about our comments, please contact Jill Sage, Quality Affairs Manager, at jsage@facs.org.

Sincerely,

David B. Hoyt

David B. Hoyt, MD, FACS
Executive Director