May 31, 2019

Don Rucker, MD
National Coordinator
Office of the National Coordinator for Health Information Technology
330 C Street, SW
Washington, DC 20201

Re: 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program [RIN 0955-AA01]

Dear National Coordinator Rucker:

On behalf of the American College of Physicians (ACP), I am pleased to share our feedback on the Office of the National Coordinator for Health Information Technology's (ONC's) 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Notice of Proposed Rulemaking (NPRM). The College is the largest medical specialty organization and the second-largest physician group in the United States. ACP members include 154,000 internal medicine physicians (internists), related subspecialists, and medical students. Internal medicine physicians are specialists who apply scientific knowledge and clinical expertise to the diagnosis, treatment, and compassionate care of adults across the spectrum from health to complex illness.

The College would first like to commend ONC for working collaboratively with the Centers for Medicare and Medicaid Services (CMS) on the publication of concurrent NPRMs focused on improving interoperability and promoting the adoption of Fast Healthcare Interoperability Resource® (FHIR) standards and standards-based Application Programming Interfaces (APIs). An essential element to drive improvements in interoperability and allow disparate health IT systems to communicate effectively is collaboration and agreement across the healthcare industry on the standards to use and how they should be implemented. The release of these parallel NPRMs, both containing proposals for the use of modern health IT standards, brings the necessary stakeholders to the table to align and improve interoperability (this includes payers, health IT vendors, physicians, patients, health information exchanges [HIEs], etc.) and improve patients' and their care teams' access to necessary health data. Given the long-standing roadblocks within the health IT marketplace for seamless data exchange, this is a necessary step to promote the use of health IT standards and hold private health care stakeholders

responsible for adherence to nationally-endorsed standards. The following discussion focuses on ACP's priority comments and concerns regarding the NPRM.

Interoperability Definition and Focus

While we appreciate ONC's thoughtful and extensive efforts to implement important elements of the *21st Century Cures Act* and promote the adoption and use of modern health IT standards and standards-based APIs, the College remains concerned around the federal government's definition of interoperability. Specifically, the College believes the definition of interoperability, as well as the implementation and measurement of interoperability initiatives, should not focus solely on high volumes of data transferred or access to every piece of health information ever collected. There remains a fundamental misconception that indiscriminately sending all data is promoting or enhancing interoperability and improving patient care. From a technical perspective, once the full set of clinical data is sent from the source, it is considered historical data. A critical piece of information may have changed since the latest copy was received that could completely change a medical decision. The current definition of interoperability described in the *21st Century Cures* legislation[1] does not recognize that accessing every aspect of a patient's information can sometimes actually hinder a clinician's ability to find useful and actionable information in a timely manner.

A health care system in which health IT is measured and graded on its ability to consistently, securely, and electronically transfer and accept an abundance of clinical information at one point in time does not meet what is necessary for secure and practical interoperability. Interoperability efforts should focus on the information involved in and needed for useful clinical management of patients as they transition through the health care system, the exchange of valuable, meaningful data at the point of care, the ability to incorporate clinical perspective, and query health IT systems for up-to-date information related to specific and relevant clinical questions**.** Moreover, ONC's current proposals contain very broad definitions of electronic health information (EHI), information blocking, and the regulated actors, as well as allow for subjective interpretations of the exceptions to information blocking, raising significant concerns for clinicians who already regularly experience information and cognitive overload when trying to find the data needed to provide high-value, patient-centered care.

Therefore, ACP strongly reiterates recommendations we have made in previous comment letters that any initiatives to improve interoperability, including those that give patients rightful access to their EHI, should be implemented through an iterative process, so that their effects on patient care, privacy, and security are adequately demonstrated and the risks of data overload and data without context are mitigated. ONC should prioritize facilitating access to meaningful patient health information by targeting the high-yield clinical data that have shown to be the most useful in current health information exchange practices.

Information Blocking Provisions – Effects on Clinician Burden

As the *21st Century Cures Act* outlined and ONC has described in detail within the NPRM, it is clear that the practice of information blocking, including charging exorbitant fees to access

[1] HR 34 21st Century Cures Act: https://www.congress.gov/114/plaws/publ255/PLAW-114publ255.pdf.

data, needs to be addressed and we appreciate the extensive work put into describing these types of activities and the exceptions to information blocking. Particularly, we are pleased with ONC's inclusion of exceptions to information blocking when preventing patient harm, privacy and security, EHR downtime for maintenance, and infeasible requests and substantial burdens.

Even provided these thorough explanations and examples, we are concerned about the burden imposed on clinicians through the implementation of these provisions. First, understanding how the complex information blocking provisions will affect our members in their daily practice will prove to be extremely complicated. Each information blocking claim or exception will be reviewed in a subjective manner and based on the facts and circumstances of each case. Second, not only are the information blocking provisions, exceptions, and sub-exceptions complicated in and of themselves, they overlap with the existing *Health Insurance Portability and Accountability Act's* (HIPAA) minimum necessary requirement and it will be difficult to understand what information a clinician is permitted versus required to share for any given individual patient. There are varying state laws around privacy as well – and these federal regulations will not supersede the state laws – adding more complexity and burden to the process. Third, with ONC, the Office of the Inspector General (OIG), and the Office for Civil Rights (OCR) all having some type of oversight and enforcement authority, there will inevitably be differences in interpretation of information blocking claims.

In order to meet these new regulatory requirements, it will take significant time and resources to develop and implement internal policies around the types of API queries the health system or physician practice will allow into their system and to make sure they are covering their bases to defend themselves against any future information blocking claims. This burden will disproportionately disadvantage independent physician practices as they likely do not have the resources to employ information security or health information management departments to assist them in deciphering the complex and overlapping regulations. For those clinicians who do not understand the complexity of the information blocking provisions, or do not have the resources to help them navigate the enforcement of these regulations, they may end up sharing more data than is necessary or required, putting sensitive health information at risk.

Moreover, throughout the NPRM, ONC promotes the goal of providing payers with access to EHI, but the information blocking provisions do not apply to payers. This could inadvertently empower payers to demand more information than is needed, as discussed above, and then claim that clinicians are information blocking if they do not comply. Clinicians, despite using their professional judgment, will then have to go through the additional steps of the privacy and security sub-exception to prove they are not information blockers.

For these reasons, ACP recommends ONC scale back the scope and definition of EHI as it relates to the information blocking provisions and focus in, at least initially, on the data elements within the proposed US Core Data for Interoperability (USCDI). The College is aware that the USCDI is a limited set of data and does not fully capture the data needed for all aspects of health care, but to our earlier discussion around the complexity of interoperability and the recommendation to proceed using an iterative process, focusing on the USCDI seems like a reasonable middle ground. Requiring the exchange of USCDI elements still addresses the policy

concern of hoarding data, and holds those bad actors accountable, but gives the industry time to upgrade systems that promote secure, safe, and practical interoperability and lessens the regulatory burden on practicing clinicians, a key priority of the administration. As part of this recommendation, patients would retain their rights to request their designated record set as described by HIPAA (and as noted in Appendix A, the EHI export functionality provision could initially focus the scope of EHI on the electronic patient health information [ePHI] outlined by HIPAA.) With that initial focus, ONC along with the necessary healthcare stakeholders' ongoing input can continue to expand the USCDI and the data that falls under the scope of EHI and information blocking claims through a consensus-based deliberative process facilitated by nationally recognized standards development organizations (SDOs).

Promotion of Health IT Standards, Standards-based APIs, and the Evolving App Ecosystem

ACP appreciates ONC's continued efforts to advance interoperability through promoting the adoption of modern interoperability standards, including FHIR®, and promoting the use of standards-based APIs. **ACP recommends ONC require the use of FHIR® Release 4 (R4) immediately instead of focusing on FHIR® Release 2 (R2) in these initial development stages.** Given that the certification updates will not happen for at least two and a half years, it is likely that FHIR® R2 will no longer be the dominant version in use. Additional comments and recommendations on the standards versioning and associated implementation guides can be found in Appendix A.

The College agrees that APIs are an important component in health information exchange and have the potential to greatly advance patients' access to their data and the exchange of information. We support the concept of patients having seamless access to their health information and have long advocated for the use of standards-based APIs to help promote EHI exchange. However, we have concerns about the API proposals related to patient privacy, security, and cost. The College is concerned that a number of patient privacy issues will arise when allowing third-party app developers to access EHI on behalf of the patient when the patient is unaware of who they are actually allowing to access their data. As proposed, ONC is not requiring API technology to include privacy controls even though the technological capability exists to do so. Recent reports[2] discuss how app developers sell data to third parties and how most do not share privacy policies with the patient or, when they do, do not adhere to those policies. Personal health information is some of the most sensitive and private information for an individual. While it is absolutely a patient's right to have access to that information, allowing and promoting access without requiring necessary privacy and security controls, presents a very real risk and will ultimately affect the patient's willingness to disclose information to his or her clinician.

As the health IT app ecosystem continues to evolve, patients need to be properly educated and provided clear guidance around what they are agreeing to when signing into an app and that their personal EHI could be at risk. **ACP recommends ONC include, as a Condition and Maintenance of Certification, a provision that vendors supplying API technology require the**

[2] Huckvale K, Torous J, Larsen ME. Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation. *JAMA Netw Open.* 2019;2(4):e192542. doi:10.1001/jamanetworkopen.2019.2542

API user, or the app developer, to have in place a model privacy notice, possibly resembling that of ONC's Model Privacy Notice.[3] This will provide a uniform and plain language description to the patient about how the information is sold so that both the app developer and the clinician can accurately reflect what is being shared, and also decrease the burden on clinicians who will have to navigate differing privacy practices across the app industry. Additionally, there needs to be some mechanism to report bad actors or app developers that consistently share data inappropriately. From the physician perspective, ACP has significant concerns that clinicians will be required to allow apps to query their systems without certainty that the app are behaving appropriately. Physicians feel a fundamental responsibility to protect their patients and their patients' information. API access coupled with the information blocking regulations should not absolve physicians or require them to ignore deeply felt professional responsibilities to their patients. **To that end, ONC should clarify within the information blocking exceptions, that a physician's professional judgment will not be considered information blocking when there is proof that the physician took action to protect information.** We are also concerned about the costs associated with installation as well as the ongoing operation of APIs. While the College supports ONC's proposals to limit the fees a vendor can charge a physician and provide patients access to data free of charge, we are concerned that physicians will be expected to provide data exchange services without being permitted to charge for these services.

We would also like to highlight that use of APIs cannot be relied upon as the only solution to issues with interoperability. The fact that there is no standard API and that a clinician interacting with multiple EHR systems is dealing with multiple APIs can lead to numerous versions of clinical data outputs – with clinical data presented in varying forms lending to the previous information overload discussion. Moreover, the API Resource Collection in Health (ARCH) – a government unique implementation specification that aims to help standardize APIs, is troublesome due to the mix of components that are not true standards**. ONC should not specify implementation guidance and specifications developed by non-standards development organizations (SDOs) through regulations. The ARCH itself should only include true standards**. Further guidance should be specified through sub-regulatory processes.

Development and Implementation Timelines

Due to the complexity of both the ONC and CMS NPRMs, there are a number of overlapping timelines that are not fully aligned and do not seem entirely feasible. For example, the CMS NPRM has more aggressive proposals for API deployment and proposes to require some health plans to support the updated functionality by January 1, 2020 – while other plans are required to do so by July 1, 2020. These compressed timeframes could result in problems in software being deployed that is not fully conformant with standards and properly tested – and could have implications on patient care.

ONC proposes, in this NPRM, a 24-month development timeline for health IT developers, which includes the implementation of upgraded technology in clinician practices. While these timeline proposals are not as compressed as the CMS proposals, they are equally concerning. Numerous

[3] ONC 2018 Model Privacy Notice: https://www.healthit.gov/sites/default/files/2018modelprivacynotice.pdf

updates to ONC's Health IT Certification program are being proposed, and it will take a significant amount of time for health IT vendors to make these upgrades – separate from the time needed to implement the upgraded systems. The College strongly reiterates our previous concerns around rushing health IT implementation timelines to meet regulatory requirements. These concerns include the significant cost associated with implementation and the large amount of time these types of system upgrades take to roll out, including effectively deploying the new technology, staff training, and workflow adjustments – all leading to potential risks to patient health. Moving to more up-to-date standards and functions is important, but it is important physicians have adequate time to train clinical staff and test and implement the upgrades once the new versions of 2015 certified electronic health record technology (CEHRT) are available from their vendors to help ensure patient safety and a smooth transition to the new technology. **To that end, the College recommends that physicians be given at least six months, if not a full year, for implementation of upgraded health IT systems once they are made available by their vendors before physicians are regulated on the use of their new technology**. ACP recommends ONC focus on the vendor development timelines and allow other HHS agencies to determine policies regarding physician adoption and use. ACP is also concerned that it will be difficult for physicians to determine which version of their 2015 edition CEHRT meets the updated requirements – as well as any confusion that will arise when meeting the requirements for CEHRT under CMS' Quality Payment Program. **ONC should clarify how to distinguish the updated 2015 CEHRT edition with the previous 2015 version – possibly by renaming the updated version to "2015 v2" or the "2019 Edition."**

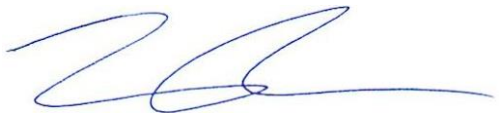
Additionally, the information blocking provisions within both proposed rules will go into effect before the technology upgrades to facilitate EHI exchange are required and safely implemented. **Therefore, vendors should be required to support an initial defined subset of data to be exported if physicians are going to be held to the information blocking provisions.**

Interim Final Rule Recommendation

The College recommends ONC consider issuing an Interim Final Rule (IFR) with an additional 30- or 60-day comment period prior to finalizing the existing NPRM. This will allow ONC to review public feedback and make final determinations on the readiness of FHIR® Release versions and related IGs. An IFR will also give ONC the option to incorporate stakeholder feedback and provide clarification on a number of provisions including the naming of the updated 2015 CEHRT edition, scope of EHI, EHI with respect to information blocking claims, among others. ONC has outlined a number of policies that have the potential to fundamentally change how health information is exchanged but it is imperative that this be an iterative process and that the risks and concerns raised through public rulemaking are addressed and/or clarified to increase the likelihood of ONC achieving its important and well-intended policy objectives.

Thank you for the opportunity to provide feedback on this extremely important set of policies and regulations. We hope you find value in our feedback. Should you have any questions, please contact Brooke Rockwern, MPH, Associate, Health IT Policy at brockwern@acponline.org.

The following Appendix A contains ACP's comments and recommendations on specific provisions within ONC's NPRM.



Zeshan A. Rajput, MD, MS
Chair, Medical Informatics Committee
American College of Physicians

I. Removal of Randomized Surveillance Requirements

Background: ONC proposes to remove the requirements to conduct randomized surveillance of certified health IT products.

ACP Comments: The College has previously expressed concerns around the effectiveness of the random surveillance program and supports the removal of this provision.

II. Updates to the 2015 Edition Certification Criteria and Standards

Background: ONC proposes a number of updates to the 2015 Edition CEHRT including removal of previous functional certification requirements, updates to existing requirements, and the addition of new certification criteria.

ACP Comments: ACP supports the proposals to remove previous functional certification requirements for EHRs (e.g., problem list, medication list, medication allergy list, smoking status, etc) and focus instead on interoperability requirements. However, while we agree that these functionalities are nearly ubiquitous across vendors, it still does not mean they are useful or usable. As the certification programs shift to focusing on interoperability or exchanging of the data captured by these functionalities, ONC should not lose sight of the usability of these widespread health IT functionalities and their ability to capture accurate and useful data. Being able to send and receive a meaningless problem list or summary of care document will not improve interoperability – and in most cases will add more burden on the physician for having to reconcile the data. **ONC should continue to critically assess the efficiency and operability of these widely adopted and used functionalities to continue to improve health IT usability, possibly through the Real-World Testing Condition and Maintenance of Certification.** For example, there are requirements on the physician to use the CancelRx transaction when e-prescribing; however, there is no requirement on the pharmacy to accept the transaction which leaves gaps and delays in the overall functionality of e-prescribing. **ONC should work with pharmacy stakeholders to promote and/or require the adoption and consistent implementation of the CancelRx transaction.**

Specific to the proposals to expand the currently limited smoking status value set, ACP is supportive of this move. The previously overly restricted value set for reporting smoking status has caused enormous problems for all participants and we greatly appreciate ONC recognizing these issues and attempting to address them through expanding the value set. Value sets, just like structural standards, must result from consensus-based deliberative processes involving all stakeholders and facilitated by SDOs.

We would like to reiterate our concerns around ONC proposing to not change the name of the upgraded 2015 edition. It will be difficult for clinicians to determine which version of their 2015 edition CEHRT meets the updated requirements – as well as any confusion that will arise when meeting the requirements for CEHRT under CMS' Quality Payment Program. **ONC must clarify**

how to distinguish the updated 2015 CEHRT edition with the previous 2015 version – possibly by renaming the updated version to "2015 v2" or the "2019 Edition."

a. Recognition of Food and Drug Administration Processes – Development of Similar Independent Program Processes – Request for Information

Background: ONC seeks comment on whether they should establish new regulatory processes tailored towards recognizing the unique characteristics of health IT (e.g., EHR software) by looking first at the health IT developer, rather than primarily at the health IT presented for certification, allowing vendors to self-certify.

ACP Comments: The College would like to raise concerns with this type of approach for certification of health IT. Due to the highly sensitive and important medical information stored within these systems, it is important that the health IT module itself is properly assessed to ensure patient safety.

b. Standards and Implementation Specifications

Background: ONC proposes the use of voluntary consensus standards (those developed through SDOs like Health Level 7® (HL7)) except for the use of:

- the United States Core Data for Interoperability (USCDI), Version 1(v1);
- the government unique ARCH Version 1 implementation specification;
- the use of other market-driven consortia standards for APIs;
- and the use of government unique standards for reporting electronic Clinical Quality Measure (eCQM) data to CMS.

ACP Comments: ACP supports the move to USCDI v1 from the Common Clinical Data Set (CCDS); however, much clarification is needed to make the USCDI implementable. There is a significant leap from specifying data classes in the USCDI to fully implementing those data classes in standards that are ready for use. Also, we have learned the hard way that implementation of data structures in standards does not result in successful interoperability. Each standard requires one or more companion implementation guides that explain to developers how to use the standards properly.

Regarding the government unique ARCH, we reiterate our comments that, as proposed, the ARCH is troublesome due to the mix of components that are not true standards. **ONC should not specify implementation guidance and specifications developed by non-SDOs through regulations. The ARCH itself should only include true standards. Additional guidance should be specified through sub-regulatory processes.**

Promoting API functionality is important, but promoting it without an industry agreed upon standard is worrisome. **We urge ONC to review the work being done at SDOs and use what they can there before allowing vendor-specific specifications for APIs.**

c. USCDI – Provenance

Background: The USCDI v1 also includes a new data class, titled "provenance" that includes three specific data elements: author, author's time stamp, author's organization. Provenance describes the metadata, or extra information about data, that can help answer questions such as when and who created the data. The inclusion of "provenance" as a data class in the USCDI v1 would also complement the Cures Act requirement to support the exchange of data through the use of APIs. Data exchange through the use of APIs allows for more granular data and differs from the exchange of data via the Consolidated-Clinical Document Architecture (C-CDA). While C-CDAs are often critiqued due to their relative "length," the C-CDA represents the output of a clinical encounter and includes relevant context. The same will not always be true when exchanging more granular data through the use of APIs. The inclusion of provenance would help retain the relevant context so the recipient can better understand the origin of the data.

ACP Comments: Provenance is another important concept to consider as health data become more available and shareable. Provenance data are included in CDA and FHIR® standards and can be attached in order to track the original source of each observation. Any data received or sent could have a marker of the origin associated with the data that would be evident to subsequent users of that information – providing great clinical value when exchanging health information and helping to mitigate any issues with inaccurate data. The key safety concern is that as data move from system to system, it is not at all clear which provenance data should be added, deleted, or revised. If vendors and implementers make different decisions regarding the management and use of provenance data, we could find ourselves with more problems than we have without provenance data. **ONC should work with stakeholders to develop industry guidance on best practices for implementing and managing provenance functionality in systems prior to requiring the exchange of provenance data.** Regarding ONC's future EHR Reporting Program criteria, every effort should be made to include reporting requirements focused on how EHR systems address mitigating inaccurate data. Transparency in this area is crucial and health IT vendor-reporting requirements should include questions around implementation and management of provenance functionality as well as questions on whether the system allows for bidirectional communication to correct data shared among clinicians and patients.

d. USCDI – Relationship to Content Exchange Standards and Implementation Specs

Background: In order to align with their approach to be responsive to the evolution of standards and to facilitate updates to newer versions of standards, the USCDI v1 is "content exchange" standard agnostic. It establishes "data policy" and does not directly associate with the content exchange standards and implementation specifications which, given a particular context, may be necessary to exchange the entire USCDI, a USCDI class, or elements within it.

ACP Comments: Currently, all data classes in the USCDI v1 cannot be supported by commonly used "content exchange" standards; however, the standards should be in a better place by the time the provisions are implemented. **This will require ONC to update the versions of**

standards that it references as it is not certain that *all* needed changes will be included in published standards by the time ONC finalizes this regulation.

e. Clinical Quality Measures (CQMs) – Report Criterion

Background: As a means of reducing burden, ONC proposes to remove the HL7 Quality Reporting Document Architecture (QRDA) standard requirements from the 2015 Edition CQMs, but require that certified health IT support the CMS QRDA IGs. ONC believes this would directly reduce burden on health IT developers and indirectly clinicians as they would no longer have to, in practice, develop (health IT developers) and support (both developers and clinicians) two forms of the QRDA standard (i.e., the HL7 and CMS forms). To support the proposal, ONC proposes to incorporate by reference the latest annual CMS QRDA IGs, specifically the 2019 CMS QRDA I Implementation Guide for Hospital Quality Reporting and the 2019 CMS QRDA III Implementation Guide for Eligible Professionals (EPs) and Eligible Clinicians. A Health IT Module would need to be certified to both standards to provide flexibility to clinicians.

ACP Comments: Some of the changes in the CMS version of the IG are there to support program-specific reporting requirements. This causes difficulties for other reporting programs such as The Joint Commission, to use the CMS version of the IG, since their reporting requirements are different. If CMS were to remove program-specific requirements from the IG, then the IG might be made useful for all reporting. CMS could move specific reporting requirements to a separate document.

f. Electronic Health Information Scope and Export Function

Background: ONC proposes to define EHI to mean "electronic protected health information (as defined in HIPAA), and any other information that:

- is transmitted by or maintained in electronic media;
- identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual;
- relates to the past, present, or future health or condition of an individual;
- the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual."

The proposed definition is not limited to information that is created or received by a clinician and does not include health information that is de-identified.

ONC also proposes a new 2015 Edition certification criterion for EHI export that would replace the previous "data export" certification requirement. The new certification criterion supports two specific use cases in which ONC believes that all EHI produced and electronically managed by a developer's health IT should be made readily available for export. The two use cases for EHI export include individual patient requests for access and clinicians transitions between health IT systems. Within these use cases, the health IT system or organization providing the data would be required to supply data definitions that would allow the receiver to interpret the data elements accurately.

ONC seeks input on EHI export criterion as well as whether the criterion should include capabilities to permit clinicians to set timeframes for EHI export, such as only the "past two years" or "past month" of EHI. ONC also discusses whether vendors should be required to continue to support the current "data export" criterion during the migration to the EHI export functionality.

ACP Comments: The College, as previously discussed, has significant concerns around the broad definition of EHI and the ability of health IT systems to actually extract everything that falls under the scope. For example, most of the other health IT systems, including intensive care unit (ICU), radiology, and laboratory systems are not yet capable of exchanging fully structured data with EHRs and it is unclear how the EHI export function will gather all of the necessary information. It is more likely that these other systems, in order to meet the EHI export and information blocking provisions, will send whatever data they have about a patient that may not be useful or clinically relevant.

While the use case for EHI export to transition between health IT systems will be useful for physicians to transition between health IT systems, we reiterate our concerns around patient privacy when considering the broad scope of EHI. Moreover, the College is not certain how useful this type of information will be to patients. **ACP recommends that the rollout of the EHI export requirements be in stages – with defined limits on the data required – so that the industry can identify unintended consequences and address them thoughtfully. For example, the EHI export requirements could focus on the ePHI as outlined in HIPAA to prioritize patient requests for information and make sure the technology is meeting the needs before expanding the scope of EHI.**

Since the information blocking provisions will go into effect after the publication of the final rule and before this functionality is required in certified systems, vendors should be required to support an initial defined subset of data to be exported if physicians are going to be held to the information blocking provisions. The regulatory requirements for information blocking need to align with the functional capability and certification requirements of certified electronic health record technology (CEHRT). Clinicians cannot be held to certain standards of information exchange when the certification requirements of the technology will not allow them to do what is expected. **To that end, we recommend ONC issue an IFR to clarify and/or narrow the scope of EHI and align the timing of information blocking provisions to when certified technology is upgraded and safely implemented.**

g. Privacy and Security Transparency Attestations – Encrypt Authentication

Background: ONC proposes modifications to the 2015 Edition privacy and security certification framework and propose to add new criteria that a health IT developer indicate whether or not their certified health IT has the capability to encrypt authentication credentials and supports multi-factor authentication. ONC is not proposing to require the health IT have the functionality present, rather, the health IT developer is attesting that the certified technology has the capability to do so.

ACP Comments: Without proper protections, the API provisions could lead to serious damage and cause patient's health data to be at risk. Third-party app developers will push patients to use their app and then be able to access the APIs of numerous health systems. There will inevitably be bad actors in this health IT app ecosystem and it is unclear how health systems or clinicians will address issues of API usage for third-party vendors. ONC and CMS need to consider and propose how to evaluate and mitigate issues that arise before allowing the ecosystem to grow, given the high risk to patient data.

III. Conditions and Maintenance of Certification – Communications

Background: ONC proposes a Condition and Maintenance of Certification that health IT developers do not prohibit or restrict communication regarding the following subjects:

- the usability of the health information technology (including error tolerance and error handling);
- the interoperability of the health information technology;
- the security of the health information technology;
- relevant information regarding users' experiences when using the health information technology;
- the business practices of developers of health information technology related to exchanging electronic health information; and
- the manner in which a user of the health information technology has used such technology.

ACP Comments: ACP is very supportive of the Communications Condition and Maintenance of Certifications and appreciates ONC's implementation of this important element of the Cures legislation. Removing vendors gag clauses that limit clinicians from sharing health IT safety and usability concerns is an extremely important element to improving both safety and usability. The College, in our comments[4] on ONC's EHR Reporting Program Criteria Request for Information (RFI), recommended health IT developers should report on how they address and resolve "near misses." Understanding and communicating how vendors handle and address medical errors is important but information is also needed on how the vendor handles issues where the CEHRT could have caused patient harm but did not. Allowing this type of information to be communicated by the end user will help improve patient safety.

IV. Conditions and Maintenance of Certification – APIs

Background: ONC proposes to require health IT developers to publish APIs that allow data to be accessed, exchanged, and used without special effort through the use of APIs or successor technology or standards, as provided for under applicable law. ONC proposes the following attributes in order to meet their interpretation of "without special effort":

---

[4] https://www.acponline.org/acp_policy/letters/acp_response_to_onc_ehr_reporting_program_criteria_rfi_2018.pdf

- **Standardized:** ONC is adopting FHIR® as the standard and requests feedback on which version. ONC proposes the API Resource Collection in Health (ARCH), which will require developers to implement 15 FHIR® resources that map to the USCDI requirements. ONC also proposes to adopt two Argonaut Implementation Guides, OpenID Connect 1.0, and SMART App Launch Framework.
- **Transparent:** Developers must publicly provide business and technical documentation of how the API works via a hyperlink that requires access without any preconditions or additional steps.
- **Pro-competitive:** Developers must abide by business practices that promote the efficient access, exchange, and use of EHI to support a competitive marketplace.
    - **Fees:** ONC significantly limits the types of fees that developers can impose related to API access. They can charge fees for their clinician customers for use of the API but are prohibited from charging a fee for the use of API tech to facilitate a patient's ability to access, exchange, or use their EHI. Permitted fees must be based on objective, verifiable criteria that are reasonably related to the cost of supplying and supporting the API.

ACP Comments: As stated previously within our priority comments and concerns, ACP appreciates ONC's continued efforts to advance interoperability through promoting the adoption of modern interoperability standards, including FHIR®, and promoting the use of standards-based APIs. **ACP recommends ONC require the use of FHIR® Release 4 (R4) immediately instead of focusing on FHIR® Release 2 (R2) in these initial development stages.** Given that the certification updates will not happen for at least two and a half years, it is likely that FHIR® R2 will no longer be the dominant version in use. Moreover, FHIR® R2 was a draft standard, while FHIR® R4 is a normative standard and has many important elements that are not present in FHIR® R2 and are necessary to promote interoperability. FHIR® R4 is bi-directional, read or write; flexible to different levels of granularity, individual data elements or whole documents, and it is backward compatible and allows developer's code to be used on new versions. As these standards continue to evolve and mature, and new versions are made available, we support ONC's approach to provide sub-regulatory guidance on newer, approved standards versions through the Standards Version Advancement Process that will better support EHI exchange, access, and use (we provide additional comments on the Standards Version Advancement Process in later sections). The College reiterates our recommendation that proper standards published by recognized SDOs have precedence over work done by other groups, such as the Argonaut Project. While the work of the Argonaut project has been useful, **ONC should reference US Core IGs, rather than Argonaut IGs, for FHIR® R4 implementation specifications. Argonaut IGs have provided early uses cases with much-needed specificity, but they are tied to FHIR® Release 2 and provide too much optionality.** It is also unclear that the Argonaut Project will continue its work in this area and therefore it is important that the process be facilitated through an SDO.

The College agrees that APIs are an important component in health information exchange and have the potential to greatly advance patients' access to their data and the exchange of information. We support the concept of patients having seamless access to their health

information and have long advocated for the use of standards-based APIs to help promote EHI exchange. However, we have some concerns about the API proposals related to patient privacy, security, and cost. The College is concerned that a number of patient privacy issues will arise when allowing third-party app developers to access EHI on behalf of the patient when the patient is unaware of who they are actually allowing to access their data. As proposed, ONC is not requiring API technology to include privacy controls even though the technological capability exists to do so. Recent reports[5] discuss how app developers sell data to third parties and how most do not share privacy policies with the patient or, when they do, do not adhere to those policies. Personal health information is some of the most sensitive and private information for an individual. While it is absolutely a patient's right to have access to that information, allowing and promoting access, without requiring necessary privacy and security controls, presents a very real risk and will ultimately affect the patient's willingness to disclose information to his or her clinician.

As the health IT app ecosystem continues to evolve, patients need to be properly educated and provided clear guidance around what they are agreeing to when signing into an app and that their personal EHI could be at risk. **ACP recommends ONC include, as a Condition and Maintenance of Certification, a provision that vendors supplying API technology require the API user, or the app developer, to have in place a model privacy notice, possibly resembling that of ONC's Model Privacy Notice.[6]** This will provide a uniform and plain language description to the patient about how the information is sold so that both the app developer and the clinician can accurately reflect what is being shared, and also decrease the burden on clinicians who will have to navigate differing privacy practices across the app industry. Additionally, there needs to be some mechanism to report bad actors or app developers that consistently share data inappropriately. From the physician perspective, ACP has significant concerns that clinicians will be required to allow apps to query their systems without certainty that the app are behaving appropriately. Physicians feel a fundamental responsibility to protect their patients and their patients' information. API access coupled with the information blocking regulations should not absolve physicians or require them to ignore deeply felt professional responsibilities to their patients. **To that end, ONC should clarify within the information blocking exceptions, that a physician's professional judgment will not be considered information blocking when there is proof that the physician took action to protect information.** We are also concerned about the costs associated with installation as well as the ongoing operation of APIs. While the College supports ONC's proposals to limit the fees a vendor can charge a physician and provide patients access to data free of charge, we are concerned that physicians will be expected to provide data exchange services without being permitted to charge for these services.

We would also like to highlight that use of APIs cannot be relied upon as the only solution to issues with interoperability. The fact that there is no standard API and that a clinician interacting with multiple EHR systems is dealing with multiple APIs can lead to numerous

[5] Huckvale K, Torous J, Larsen ME. Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation. *JAMA Netw Open.* 2019;2(4):e192542. doi:10.1001/jamanetworkopen.2019.2542

[6] https://www.healthit.gov/sites/default/files/2018modelprivacynotice.pdf

versions of clinical data outputs – with clinical data presented in varying forms lending to the previous information overload discussion as well as our concerns with the ARCH. ACP also has concerns with the complicated fee proposals in which clinicians are expected to pay for the installation and ongoing operation of APIs without being permitted to charge for these services. Clinicians are the only regulated actors under the information blocking provisions who will not be able to recoup the cost of sharing information. Additionally, there have been recent reports from application developers that there are exorbitant costs associated with running their applications on some of the larger EHR systems.

V. Conditions and Maintenance of Certification – Real World Testing

Background: The *Cures Act* requires, as a Condition and Maintenance of Certification under the Program, that health IT developers have successfully tested the real-world use of the technology for interoperability in the type of setting in which such technology would be marketed.

ACP Comments: ACP has advocated for real-world testing of health IT and are supportive of this aspect. Production testing more accurately replicates clinical environments and patient interactions that may not occur in a controlled, non-production testing environment, ensuring health IT operates as its designers intended it to. Additionally, testing in a clinical setting gives insight into its usability by observing how the health IT performance and response time impacts workflow in its day-to-day use. While real-world production testing is important, projects of this scale are a difficult undertaking and likely why the ONC-initiated random surveillance approach was not successful. This type of vendor-driven, condition and maintenance of certification, may give this process more weight than if ONC were to randomly come into the hospital system for production testing. As mentioned previously, in addition to new standards and emerging functionalities, **ONC should continue to critically assess the efficiency and operability of widely adopted and used functionalities, like problem lists and medication lists, to continue to improve health IT usability for frontline clinicians.**

a. Standards Version Advancement Process

Background: As part of the real world testing Condition of Certification, ONC proposes flexibility within the Maintenance of Certification referred to as the Standards Version Advancement Process. The Standards Version Advancement Process would permit health IT developers to voluntarily use in their certified Health IT Modules newer versions of adopted standards so long as certain conditions are met, not limited to but notably including successful real world testing of the Health IT Module using the new version.

ACP Comments: ACP supports the Standards Version Advancement Process but emphasizes the need for ONC to work closely with vendors and clinicians through the process to address the details necessary for the process to be successful.

VI. Information Blocking

Background: The information blocking proposals define and create possible penalties and disincentives for information blocking in very broad terms. ONC proposes a set of regulated actors including clinicians or clinician groups, health IT developers of certified health IT, health information exchanges, and health information networks. ONC proposes substantial penalties, including civil money penalties, and disincentives for those who are deemed information blockers. Additionally, ONC proposes seven exceptions and sub-exceptions to information blocking: preventing harm, promoting the privacy of EHI, promoting the security of EHI, recovering costs reasonably incurred, responding to requests that are infeasible, licensing of interoperability elements on reasonable and non-discriminatory terms, maintaining and improving health IT performance. ONC proposes to implement a standardized process for the public to submit information blocking complaints while the HHS Office of the Inspector General (OIG) will be charged with enforcing the information blocking accusations.

ACP Comments: As described in detail in our priority comments, ACP has significant concerns regarding the complexity of the information blocking provisions and how it will affect our members in their daily practice. Each exception or information blocking claim will be reviewed in a subjective manner and based on the facts and circumstances of each case. Not only are the information blocking provisions, exceptions, and sub-exceptions complicated in and of themselves, the provisions conflict with existing HIPAA minimum necessary requirement and it will be unclear what information a clinician is permitted versus required to share for any given individual patient. There are varying state laws around privacy as well – and these federal regulations will not supersede the state laws – adding more complexity and burden to the process, and with ONC, the OIG, and the OCR having some type of oversight and enforcement authority, there will inevitably be differences in interpretation of information blocking claims.

In order to meet these new regulatory requirements, it will take significant time and resources to develop and implement internal policies around the types of API queries the health system or physician practice will allow into their system and to make sure they are covering their bases to defend themselves against any future information blocking claims. This burden will disproportionately disadvantage independent physician practices as they likely do not have the resources to employ information security or health information management departments to assist them in deciphering the complex and overlapping regulations. For those clinicians who do not understand the complexity of the information blocking provisions, or do not have the resources to help them navigate the enforcement of these regulations, they may end up sharing more data than is necessary or required, putting sensitive health information at risk.

Moreover, throughout the NPRM, ONC promotes the goal of providing payers with access to EHI, but the information blocking provisions do not apply to payers. This could inadvertently empower payers to demand more information than is needed, as discussed above, and then claim that clinicians are information blocking if they do not comply. Clinicians, despite using their professional judgment, will then have to go through the additional steps of the privacy and security sub-exception to prove they are not information blockers.

For these reasons, ACP recommends ONC scale back the scope and definition of EHI as it relates to the information blocking provisions and focus in, at least initially, on the data elements within the proposed USCDI. The College is aware that the USCDI is a limited set of data and does not fully capture the data needed for all aspects of healthcare, but to our earlier discussion around the complexity of interoperability and the recommendation to proceed using an iterative process, focusing on the USCDI seems like a reasonable middle ground. Requiring the exchange of USCDI elements still addresses the policy concern of hoarding data, and holds those bad actors accountable, but gives the industry time to upgrade systems that promote secure, safe, and practical interoperability and lessens the regulatory burden on practicing clinicians, a key priority of the administration. As part of this recommendation, patients would retain their rights to request their designated record set as described by HIPAA (and as noted earlier, the EHI export functionality provision could then re-focus the scope of EHI on the ePHI outlined by HIPAA.) With that initial focus, ONC along with healthcare stakeholders' ongoing input can continue to expand the USCDI and the data that falls under the scope of information blocking claims.

VII. Patient Matching RFI

Background: ONC seeks input on additional opportunities that may exist in the patient matching space and ways that ONC can lead and contribute to coordination efforts with respect to patient matching. The Agency is particularly interested in ways that patient matching can facilitate improved patient safety, better care coordination, and advanced interoperability.

ACP Comments: Absent a national patient identifier, ACP supports a national initiative that explores the use of a common set of data elements to match a patient to his/her individual EHI. However, ACP is concerned that this may require the use of a relatively large set of identifiable patient demographic data to support matching. We believe this dependence on so many data elements may present another privacy risk for all patients.

Accordingly, ACP believes that use of a Voluntary Universal Unique Healthcare Identifier that patients could opt in to could provide privacy benefits and that its potential use should be studied. Accurate identification of patients and accurate association of patients with their data is a safety issue. A voluntary universal unique identifier for patients that has no other use beyond associating them with their health records might be less risky than using a set of demographic information that could have value beyond identification for health care purposes. We believe that this issue should not be dismissed without thorough evaluation of the potential risks and benefits. **Therefore, the College strongly recommends that HHS and ONC initiate a thorough study of the risks and benefits of a voluntary universal unique patient identifier.**

ONC begins to address some of the complexities of patient identification and matching within the newly released second draft of the Trusted Exchange Framework and Common Agreement (TEFCA) and the recommendations for qualified health information networks (QHINs) should be considered moving forward. Also, ACP recommends ONC review the work that Integrating the Healthcare Enterprise (IHE) has been doing around patient identification. ACP is a sponsor of the IHE Patient Care Coordination (PCC) domain which was established in 2005 to deal with

integration issues that cross clinicians, patient problems or time. It deals with general clinical care aspects such as document exchange, order processing, and coordination with other specialty domains. PCC also addresses workflows that are common to multiple specialty areas and the integration needs of specialty areas that do not have a separate domain within IHE.

VIII. Price Information/Transparency RFI

Background: ONC seeks comment on the parameters and implications of including price information within the scope of EHI for purposes of information blocking. In addition, the overall Department seeks comment on the technical, operational, legal, cultural, environmental and other challenges to creating price transparency within health care.

ACP Comments: The College supports transparency of reliable and valid price information, expected out-of-pocket costs, and quality data that allows consumers, physicians, payers, and other stakeholders to compare and assess medical services and products in a meaningful way. However, before this information is included within the scope of an already extremely broad definition of EHI, there are a number of concerns and caveats that need to be addressed when promoting price transparency. The complexity of medical billing can make it difficult or misleading to come up with a standard or average price for a particular service. Prices can vary widely based on information unique to the individual patient and visit, including comorbidities, necessary follow-up care or tests, and site of service, among a range of other factors. Pricing for self-pay patients and those privately insured are determined through two distinct processes that would require separate approaches to price transparency. Moreover, the Medicare reference price is not going to be applicable to most, and might serve to add more confusion than be useful. ACP recommends that price estimates be available prior to scheduling (i.e., at the point of sale) and that all costs are reflected (including coinsurance, deductible, etc.) to provide as much relevant and context-rich information as possible. **A critical element to promoting price information transparency is cooperation and agreement amongst the health IT vendor, health system or physician organization, and the payer.**

Beyond that, individual hospital-payer contracts can bundle services, treatments, and drugs completely differently, making direct, national, or even regional price comparisons difficult. What matters most to the patient is not the total cost of a service; it is their own out-of-pocket responsibility. **Health plans are in the best position to communicate important coverage information that impacts their customers' total out of pocket cost.** The College urges HHS to encourage health plans to share information with clinicians and patients regarding important coverage, cost, and quality information, such as whether a clinician is in-network or out-of-network. Integrating cost, quality, and coverage data into EHRs, quality clinical data repositories, regional health information exchanges, or all payer claims databases, would help physicians to be more effective partners in helping patients to navigate this information and make informed, cost-effective decisions about their care. The growing prevalence of narrow network plans exacerbates this problem and should be separately studied and addressed.

Pricing for similar services could vary across states and ACP supports national- and state-level efforts to prohibit "gag clauses" and similar contractual arrangements that interfere with the

transparency of relevant health data. ACP supports the development of alternative payment models (APMs) which show promise in aligning financial incentives to facilitate enhanced communication and coordination between multiple clinicians and cost-effective referral patterns to high-value, in-network clinicians.

Price should never be used as the sole criterion for selecting a physician or service; it should always be accompanied by quality information critical to understanding the total value of care, such as metrics about patient safety and health outcomes. If not, patients may simply defer to the lowest-cost clinicians, which could put them in a vulnerable position. At the same time, quality data released should be thoroughly vetted before being released to the public so as not to adversely penalize clinicians who care for vulnerable patient populations that are predisposed to worse outcomes, and to not further exacerbate existing social determinants of health. All information should be communicated in a readily accessible way to patients at all levels of health literacy and presented in a way that clearly articulates which services, treatments, and prescription drugs are included (and not included) in a given price, so that patients can make meaningful comparisons across settings of care and clinicians. Patients should also be made aware of the possibility of added costs due to common complications or add-on treatments. Releasing pricing information that is taken out of context, flawed, or incomplete has the potential to be more harmful to patients than lack of information.

As HHS looks to possibly regulate in this complex and sensitive pricing environment with the potential for wide-reaching implications on payers, clinicians, and patients alike, **the College recommends a graduated, targeted approach to any new price transparency initiatives and frequent consultation with stakeholders throughout the process.** Gradual implementation will help to minimize the potential for major disruptions to physician payments and therefore patient care.

IX. Disincentives for Health Care Clinicians - Request for Information

Background: Any clinician determined by the OIG to have committed information blocking shall be referred to the appropriate agency to be subject to appropriate disincentives using authorities under applicable federal law, as the Secretary sets forth through notice and comment rulemaking. ONC requests additional information on disincentives, or if modifying disincentives already available under existing HHS programs and regulations would provide for more effective deterrents.

ACP Comments: Regarding the types of disincentives to information blocking, instead of penalties, ONC and CMS should focus more on providing clinicians with education if they are found to be information blocking—much like what CMS is doing with their new auditing process for billing. If physicians are found to be information blockers, they should be provided educational tools and resources to better understand the issue prior to any disincentives (e.g., not being able to participate in Medicare).

X. Registries RFI

Background: ONC seeks information on how health IT solutions and the proposals throughout this rule can aid bidirectional exchange with registries for a wide range public health, quality reporting, and clinical quality improvement initiatives. They are also interested in feedback on use cases where an API using FHIR® Release 4 might support improved exchange between a clinician and a registry. Specifically, how the use of FHIR® R4 might:

- Reduce the burden of implementing multiple solutions for various types of exchange, while still supporting the variability needed to exchange information with registries devoted to the care of a population defined by a particular disease, condition, exposure, or therapy;
- Allow for the collection of detailed, standardized data on an ongoing basis for medical procedures, services, or therapies for particular diseases, conditions, or exposures;
- Support an overall approach to data quality, including the systematic collection of clinical and other health care data, using standardized data elements and procedures to verify the completeness and validity of those data;
- Improve and enhance the ability of clinicians to leverage feedback from a registry to improve patient care; and
- Address a sufficiently wide range of use cases to warrant the prioritization of technical innovation on API-based options over the continued development of use-case-specific solutions in future rulemaking.

ACP Comments:
As we have noted throughout this comment letter, ACP supports the use of the FHIR® standard and recommends the use of FHIR® R4 which has a strong focus on fast and easy implementation, "out-of-the-box" claims interoperability, and ontology-based analysis with formal mapping for correctness – all of which would make information more reliable and efficient to use by clinicians. FHIR® R4, with its resources for administrative concepts as well as a wide variety of clinical concepts, would be very useful from the registries standpoint for seamless and reliable data exchange. ACP looks forward to the resources and repositories of FHIR® to enhance the care delivery experience for clinicians and improve patient outcomes. Looking ahead, FHIR® R5 will include capabilities to access a complete patient record and further ongoing work to improve mapping to standard terminologies will be beneficial from the registry perspective.

The College agrees that bidirectional information flow is extremely important and we have heard from our members that they want quality performance feedback pushed into their EHR or the ability to execute actions while they are working within the registry interface – like the ability to send a reminder to a patient who is not meeting certain performance criterion. ACP held a focus group with members involved in our Quality Improvement programs and concerns were raised about not trusting the data they receive from performance feedback platforms. As efforts to improve bidirectional information flow move forward, it is critical that more reliable data feed to registries and that the end users get meaningful and timely feedback that is trustworthy.

Regarding the use and expansion of the USCDI, ACP recommends that ONC work in collaboration with the QCDR community and other clinical data registry groups, in addition to the annual public comment period on the USCDI, to incorporate specific registry-related data classes and data elements into the USCDI. ONC needs to hear directly from registry and public health groups to better understand the complexities needed for data exchange and we believe the public comment process alone is not sufficient. Also, since patient engagement and feedback is core to quality improvement, the College recommends ONC work to include patient-related data classes and elements, including data on social determinants of health.