



## Sound Policy. Quality Care.

June 3, 2019

Don Rucker, MD  
National Coordinator for Health Information Technology  
Office of the National Coordinator for Health Information Technology  
U.S. Department of Health and Human Services  
330 C Street, SW  
Washington, DC 20201

Submitted electronically via <http://www.regulations.gov>

**RE: 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Proposed Rule (RIN 0955-AA01)**

Dear Dr. Rucker:

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

Both rules aim to accelerate game-changing innovation aimed at minimizing errors, improving care coordination, reducing clinician burden, lowering costs, and enhancing consumer experience. The Alliance strongly supports these goals and has no doubt that many of the proposals in the ONC rule will accelerate progress towards a more interoperable healthcare system. However, if the numerous new and complex requirements set forth in this rule are implemented too rapidly, it will result simply in a proliferation of poorly functioning products as the industry shifts its focus to solely satisfying the parameters of this rule rather than developing features that serve markets such as specialty medicine. Furthermore, the Alliance also has serious concerns that if data is unleashed too rapidly and without adequate standards, parameters, and context, it will be uninterpretable to patients and at considerable risk for misuse. If the goal is to make patients better healthcare consumers and to provide clinicians with information that will lead to more appropriate and efficient care, then it is critical for both CMS and ONC to carry out these reforms carefully and gradually. If the infrastructure is not first in place to minimize these risks, then this surge of data will simply overwhelm patients and the clinicians who care for them and potentially be misapplied in ways that impact coverage, access to care, and the physician-patient relationship.

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

## Executive Summary

- **2015 Edition Certification Criteria**
  - The Alliance recommends that ONC update the name of the 2015 Edition Certification criteria (e.g. “2019 Edition Certification Criteria” or “2015 Edition Certification Criteria 2.0”) to reflect the multiple significant proposed changes in this rule.
- **Electronic Health Information (EHI) Export**
  - The Alliance strongly supports the goal of the EHI export proposal, but recommends that the export requirement only apply to electronic protected health information (ePHI) as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) rather than the more expansive definition of EHI proposed in this rule.
  - We recommend that ONC consider adopting standards that certified health IT developers would have to adhere to ensure that data can not only be exported, but also imported by the receiving entity.
  - We request that ONC clarify the intersection between its data export proposal and its Application Programming Interface (API) proposals, including the extent to which APIs would facilitate data export.
  - We urge ONC to continue to work with stakeholders to accelerate the incorporation of Digital Imaging and Communications in Medicine (DICOM)-based images into certified health IT, into the U.S. Core Data for Interoperability (USCDI) standards, and into the nation’s broader interoperability framework.
- **Conditions and Maintenance of Certification**
  - The Alliance supports the use of Conditions and Maintenance of Certification requirements under the Certification Program since they would establish clear baseline technical and behavior requirements, as well as ongoing requirements that these conditions are continually being met by both health IT developers and their certified products.
  - We request that ONC strengthen the Real World Testing provision to require that developers test their products within the specialty to which the technology would be marketed.
  - The Alliance recognizes the value of Application Programming Interfaces (APIs), but strongly urges HHS to carefully evaluate the potential implications associated with making data so easily accessible and transferable, including risks related to information overload, data security, and increased physician burden.
    - It is critical that HHS carefully re-evaluate current regulatory policies, including the reach of HIPAA, in the context of modern data exchange to ensure privacy and security protections for health information keep up with the pace of technology.
    - Regulations also must evolve to reflect the additional demands that will be placed on physicians as a result of the enhanced data access.
    - It is equally important that federal agencies provide clear guidance to physicians about their obligations under this shifting landscape.
    - Clearer guidance is needed to ensure that Health IT developer charges are truly reasonable and that providers, who are already required to buy and upkeep this technology, are not responsible for costs outside of their control. Providers should not be held responsible for costs that they have little or no control over, such as costs related to the frequency with which their patients rely on the provider’s API technology to access their records.

- **Information Blocking**
  - It is critical that ONC educate physicians and other stakeholders on how to navigate the fine balance between HIPAA, which dictates that physicians not share data unless they have a permissible purpose, and the information blocking rules, which dictates that physicians must share data unless they meet an exception. We strongly recommend that ONC focus first on effective education rather than effective deterrents or disincentives.
  - The Alliance believes that the definition of EHI is too broad and subjective for the purposes of enforcing information blocking. We recommend that the information blocking provisions only apply to the data classes in the USCDI, which aligns with the API certification requirements proposed in this rule.
  - We believe it is unreasonable to include registries in the list of actors that would be regulated by the information blocking provisions and to hold registries accountable for ensuring that patient-specific data is easily and regularly accessible to the patient or a third-party requestor.
  - It is important that health plans are included on the list of regulated actors since health plans manage huge amounts of data on individual patients and would be required, under the CMS rule, to share such data with patients and providers.
  - We strongly urge ONC to provide physicians with more clarity on information blocking, including guidance documents with additional specific examples of what does constitute information blocking and clear instructions on steps physicians can take to avoid being accused of it. It also is critical that ONC adopt clear and consistent criteria for evaluating information blocking complaints and adhere to a transparent process for vetting such complaints. ONC must provide assurances that if a physician tries, in good faith, to comply with an exception or otherwise not engage in information blocking, that ONC would strongly consider such evidence in assessing an allegation of information blocking.
- **Price Transparency RFI**
  - HHS needs to proceed cautiously in this area. It must remain mindful of the unique nuances that factor into healthcare decision-making and work to ensure that patients understand their full range of options and the potential implications of each of those options. Payers— not physicians— should be responsible for releasing price information and presenting it in a way that is useful for the patient.
- **Registries RFI**
  - The Alliance believes that ONC’s proposed standards for certified APIs, as well as its proposed restrictions on information blocking, have the potential to improve how information is exchanged with registries.
- **RFI on Patient Matching**
  - The Alliance appreciates that ONC is looking into alternative solutions to this ongoing problem. Solutions should not exacerbate current challenges and lead to more errors or increased administrative burden.

## Detailed Comments

### Updated 2015 Certification Criteria

***Since ONC proposes multiple significant updates to its 2015 Edition Certification Criteria, we recommend that it also update the name of these criteria (e.g. “2019 Edition Certification Criteria” or “2015 Edition Certification Criteria 2.0”) to reflect these changes.*** An updated name would minimize confusion among clinicians about which Edition they should invest in and/or which Edition would allow them to most easily comply with new interoperability standards, as well as the Promoting Interoperability requirements of the Merit-Based Payment System (MIPS).

### EHI Export

ONC proposes to require, through updated 2015 Edition certification criteria, that health IT developers provide the capability to electronically export all electronic health information (EHI) that they produce and electronically manage in a computable format. Specifically, this criterion would:

- Enable the export of EHI for a single patient upon a valid request from that patient or a user on the patient’s behalf;
- Support the export of EHI when a health care provider chooses to transition or migrate information to another health IT system; and
- Require that the export include the data format, made publicly available, to facilitate the receiving health IT system’s interpretation and use of the EHI to the extent reasonably practicable using the developer’s existing technology.

ONC clarifies that EHI export encompasses all the EHI that the health IT system produces and electronically manages for a patient or group of patients. This applies to the health IT’s entire database, including but not limited to clinical, administrative, and claims/billing data. “EHI” also includes the oldest EHI available on that patient to the most recent, no matter the specific electronic format (e.g., PDFs are included). ONC proposes that health IT developers must implement this capability within 24 months of the final rule’s effective date.

***The Alliance strongly supports the goal of this proposed criterion, which is to provide patients and health IT users— including providers— a means to efficiently export the entire electronic health record for a single patient or all patients in a computable, electronic format.*** In conjunction with the data blocking provisions, this new criterion would provide some degree of assurance that a health IT developer supports, and does not inhibit, the access, exchange, and use of EHI for the specific use cases that the criterion addresses. Although we fully support requiring developers to build systems that can readily export data produced and electronically managed by the health IT as a standard capability of certified health IT, we also have concerns that this is too aggressive of a goal to accomplish within a 24-month timeframe. If deployment is rushed, it could result in poor functionality, cumbersome user-interfaces, and inflated costs for clinicians. ***Given these risks, the Alliance recommends that the export requirement only apply to electronic protected health information (ePHI) as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) rather than the more expansive definition of EHI proposed in this rule (see comments related to EHI in Information Blocking section below).*** This will provide health IT developers with a more manageable mandate and help to minimize potential unintended consequences that could interfere with the goals of this proposal. Understanding that developers are not able to export every existing data element, nor that all possible data elements are necessary for transfer, ONC also seeks comment on whether, in the future, it should

require that health IT developers attest or publish as part of the export format documentation the types of EHI they cannot support for export. ***While the Certification Program should continue to put pressure on health IT developers to make as much data as is feasible available for electronic export, we support this proposal as an interim solution that would enhance transparency and assist physicians when deciding which systems to invest in.***

In this section, ONC also clarifies that the clinical data that would have to be made available for export would encompass imaging information – both images and narrative text about the image. However, ONC understands that EHRs may not be the standard storage location for images and solicits comment on the feasibility, practicality, and necessity of exporting images and/or imaging information. ***The Alliance believes that it absolutely critical that ONC continue to work with stakeholders to accelerate the incorporation of Digital Imaging and Communications in Medicine (DICOM)-based images into certified health IT, into the USCDI, and into the nation’s broader interoperability framework.*** 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, specialists need easier access to the image, itself, if they are to become better stewards in regards to imaging resource use and appropriate care.

Finally, ONC is not proposing that the export must be executed according to any particular standard; it is only requiring that the export must be accompanied by the data format, including its structure and syntax, to facilitate interpretation of the EHI therein. While this proposal is intended to encourage innovative export capabilities among developers, a lack of standards could potentially cause disruptions in regards to transferring EHI between EHR systems or between EHRs and registries. Also, this proposal only focuses on the ability of systems to export data, but it does little to guarantee that receiving systems can accept the data. ***We recommend that ONC consider adopting standards that certified health IT developers would have to adhere to ensure that data can not only be exported, but also imported by the receiving entity. We also request that ONC clarify the intersection between its data export proposal and its Application Programming Interface (API) proposals (discussed below), including the extent to which APIs would facilitate data export.***

### **Conditions and Maintenance of Certification**

In alignment with Section 4002 of the Cures Act, ONC proposes to establish Conditions and Maintenance of Certification requirements for the HIT Certification Program. Currently, requirements for certification are established by standards and criteria that are enforced through lab testing and in the field surveillance of products. If these requirements are not met, then the health IT developer may no longer be able to participate in the Program and/or its certified health IT may have its certification terminated. ***The Alliance supports the use of Conditions and Maintenance of Certification requirements under the Certification Program since they would establish clear baseline technical and behavior requirements, as well as ongoing requirements that these conditions are continually being met by both health IT developers and their certified products.***

The proposed Conditions and Maintenance of Certification requirements cover critical aspects of a health IT developer’s product and services, including:

#### Information Blocking

We especially appreciate that these Conditions and Maintenance of Certification requirements would

focus on prohibiting health IT developers from taking any action that institutes information blocking. As we discuss below, information blocking is a real problem that impacts specialists on a regular basis.

### Communications

We also support the Condition of Certification that would prohibit health IT developers from using gag clauses that restrict communications about the usability, interoperability, or security of their products or business practices that interfere with the exchange of electronic health information. Current developer practices often limit health IT users from openly discussing or sharing their user experiences. This proposal will promote greater transparency and open dialogue, which will help put pressure on developers to improve their systems.

### Real World Testing

This Condition of Certification would require health IT developers to annually submit real world testing plans and retrospective test results that include interoperability criteria. ONC proposes that health IT developers must real world test their products prior to the effective date of the final rule and provide real world tested health IT to all their customers within 24 months of the final rule's effective date.

The Alliance thanks ONC for requiring health IT developers to submit real world testing plans annually and retrospective test results that include interoperability criteria. We are particularly pleased that ONC emphasizes that health IT developers must test their products in the type of setting in which such technology would be marketed. ***We request that ONC strengthen this provision to require that developers test their products within the specialty to which the technology would be marketed. Lack of access to relevant specialty functionalities in certified health IT products is an ongoing problem for our members.***

### Application Programming Interfaces (APIs)

As mandated under the Cures Act, ONC would require as a Condition of Certification that health IT developers publish HL7® FHIR®-based Application Programming Interface (API) that allow health information from such technology to be accessed, exchanged, and used without special effort, as provided for under applicable law. Through the APIs, a developer must provide access to all data elements (i.e., the USCDI v1) of a patient's EHR to the extent permissible under applicable privacy laws. Other requirements include:

- APIs must adhere to standards that would enable and support persistent user authentication and app authorization processes;
- API Technology Suppliers must support API-enabled services for data on a single patient and multiple patients;
- API Technology Suppliers must publish the terms and conditions applicable to their API technology, including fees, and any other documentation necessary to interact with their APIs.

ONC proposes that API Technology Suppliers must develop, test, certify and make APIs available to their customers within 24 months of the final rule's effective date. Physicians would also be required to deploy new APIs in their clinics within the same 24-month timeframe.

As we expressed in our letter to CMS, the Alliance recognizes the value of APIs in terms of greater patient empowerment over healthcare decisions; establishing points of communications between

systems and stakeholders, which allow for the more efficient exchange of information; and enhancing interoperability. **However, we strongly urge both ONC and CMS to carefully evaluate the potential implications associated with making data so easily accessible and transferable, including risks related to information overload, data security, and increased physician burden.** Some of these implications are discussed below.

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

Given our concerns about information overload, we appreciate ONC's proposal that APIs must rely on FHIR®-based technical standards and the United States Core Data for Interoperability standard (USCDI v1) content and vocabulary standards for clinical data classes. 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 efforts to make sense of the information. In regards to the USCDI, we generally support this standard and appreciate ONC's intent to update and expand this set of data classes on an annual basis based on public input. As ONC continues this work, we **strongly urge it to incorporate Digital Imaging and Communications in Medicine (DICOM)-based images into the USCDI, into the health IT certification process, and into the nation's broader interoperability framework.** 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, specialists need easier access to the image, itself, if they are to become better stewards in regards to imaging resource use and appropriate care.

Another major concern of the Alliance is that patients might not understand that many entities that currently collect personal health information, such as fitness trackers or apps used to regulate blood pressure, fall outside the scope of the HIPAA, which could put their health data at risk. Even if patients understand these risks, it may be challenging for them to determine whether a healthcare application allows them to securely download, view, store, and share their data. The Alliance appreciates HHS' clarification that "covered entities," such as payers and providers, would not be responsible under HIPAA for the security of PHI once it has been received by a third-party application chosen by the

patient. However, these policies do not address the fact that an increasing number of organizations, which are not subject to the same rules concerning the protection of PHI as are other covered entities, are now collecting, storing, and transmitting health data.

The ONC recognized, as early as 2016, that there is a “lack of clear guidance around consumer access to, and privacy and security of, health information collected, shared, and used by non-covered entities.”<sup>1</sup> With no consistent standards for the protection of health information for these non-HIPAA covered entities, patients face a high risk of having their health data exposed, stolen, or misused. The Alliance is also concerned that payers and third-party entities may inappropriately use aggregated data gathered from patient’s records to draw potentially inaccurate and unreliable conclusions about clinician performance or that insurers may use patient health information collected through apps to limit/exclude coverage for certain services. While these might not be HIPAA issues, it is important that the federal government set parameters for the appropriate use of data by third-party entities. ***The Alliance believes that the time has come for the federal government to carefully re-evaluate the reach of HIPAA in the context of modern data exchange. Privacy and security protections for health information must keep up with the pace of technology and include minimum guidelines that apply to the influx of non-covered entities now managing ePHI.*** We are supportive of the direction ONC seems to be taking in the updated draft of its Trusted Exchange Framework and Common Agreement, which requires non-HIPAA entities, who elect to participate in exchange, to be bound by certain provisions that align with safeguards of the HIPAA Rules. The Alliance agrees with ONC that this will bolster data integrity, confidentiality, and security, which is necessary given the evolving landscape. ***Similarly, we believe that ONC should establish an appropriate security controls framework for interoperability and data sharing, including a strategy to ensure that third-party apps properly authenticate for EHI use and do not improperly modify or use a patient’s medical record.***

As we expressed in our comments to CMS, the Alliance also believes that federal agencies have an obligation to work together to assist with education and to set standard terms and conditions that would make it very clear to patients what they are agreeing to, how their information could be used, which organizations are required to comply with HIPAA and which are not. These duties should not fall on the shoulders of providers. It is also important for federal agencies to educate the physician community about these new data sharing risks, as well as what role and obligations the physician has in terms of making data available, authenticating the identity of requestors of data, and otherwise authorizing access to data. ***In summary, it is critical that federal agencies work together to conduct an aggressive educational campaign to clearly explain to patients the implications of sharing their data with third-party entities that are not non-covered entities and the potential for data to be potentially commoditized or misused in ways that can impact coverage, access to care, and interfere with the physician-patient relationship. It is equally important that federal agencies provide clear guidance to physicians about their obligations under this shifting landscape.***

In this section of the rule, ONC also proposes specific conditions that would set boundaries for the fees API Technology Suppliers (i.e., health IT developer that create API technology presented for certification) would be permitted to charge and to whom those fees could be charged. Our interpretation of these proposed policies is that, consistent with the data blocking restrictions discussed later in this rule, the API User (i.e., the patient) cannot be charged for access to the API software. However, the API

---

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

Technology Supplier can recover documented and non-discriminatory costs for developing and upkeeping the technology per an agreement with the API Data Provider (i.e., health care providers who purchase or license API technology and provide access via the API technology to data they produce and electronically manage). The API Technology Supplier also can license the use of API technology they create to recoup costs and potentially make a profit. Additionally, API Technology Suppliers would be permitted to charge API Data Providers based on the post-deployment usage activities of API Users.

The Alliance is concerned about these policies since they place costs squarely on the shoulders of providers who are essentially mandated to use certified EHRs that include API technology and to provide patients with access to data via those APIs. Similarly, it is unreasonable to presume that API User-driven data overages should be the responsibility of the API Data Provider. As ONC acknowledges in the rule, this pricing model is open to abuse, with API Data Providers at risk of paying unreasonably high fees if the volume of API use is high. **Providers already must invest significant resources to adopt and maintain certified EHR technology. They should be recognized for this investment and for making API technologies available to patients. They should not be held responsible for costs that they have little or no control over, such as costs related to the frequency with which their patients rely on the provider's API technology to access their records.**

Health IT developers are expected to considerably increase the price of their CEHRT products to cover the cost of complying with all of the new requirements set forth in this rule. ONC clarifies in this section that “the API Technology Supplier would need to be careful to ensure that the total fees paid by an API Data Provider were reasonably related to the API Technology Supplier’s costs of supporting the API technology. Where the fees paid over a reasonable measuring period were not reasonably related to the API Technology Supplier’s costs, they would not be permitted.” While we appreciate this disclaimer, these statements rely on vague terminology that can be interpreted widely. **Clearer guidance is needed to ensure that Health IT developer charges are truly reasonable and that providers, who are already required to buy and upkeep this technology, are not responsible for costs outside of their control.**

We also request clarification on the following statement: “Any fee that arises in connection with an API User’s use of API technology would need to exist solely between the API Data Provider and the API User.” This seems to suggest that there might be situations when an API Data Provider can, in fact, pass on some of these costs to API Users. **We would appreciate if ONC could more clearly explain when it is (and is not) appropriate for an API User to be charged a fee in connection with use of API technology.**

Finally, the Alliance opposes ONC’s decision to propose a single date by which API Technology Suppliers and API Data Providers must deploy upgraded API technology. Not only is this implementation timeline aggressive, but it is unreasonable to expect physicians to have the ability to deploy upgraded APIs in their clinic within the same 24-month timeframe as API Technology Suppliers are required to deploy their upgraded technology. API Technology Suppliers should be provided a specific timeline to develop, test, certify, publish, implement, and train their customers on new product features and functions. This timeline should be separate from physician adoption requirements. If ONC continues with its proposal it should, at the very least, provide physicians additional implementation time beyond 24 months.

### **Information Blocking**

The Cures Act defines information blocking broadly as any practice that is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information (EHI) when the entity knows it is likely to do so. Under the Cures Act, the general prohibition on information

blocking applies to health care providers, developers of certified health IT, health information exchanges, and health information networks. In this section, ONC defines EHI and defines the “actors” to which these restrictions apply, thereby establishing the scope of who and what is covered by the information blocking provisions. ONC also provides a list of activities that would be likely to interfere with access, exchange, or use of EHI, proposes seven exceptions to the general prohibition on information blocking, and issues an RFI on potential “disincentives” for health care providers who engage in information blocking.

Despite rights afforded under HIPAA, patients still struggle to access their health information, to transfer their records from one provider to another, and to get all of their information in one place. Physicians also continue to face significant challenges related to data access, including EHR vendors “locking-up” data in non-portable formats or charging exorbitant fees to establish interfaces that allow physicians to access their own data in a user-friendly manner, or to share data with another EHR system or clinical data registry. Hospitals and health systems also often interfere with the sharing of data through contractual arrangements or by inappropriately claiming the need to comply with the HIPAA Rules. Given these ongoing obstacles, the Alliance greatly appreciates ONC’s multi-pronged approach to encouraging more coordinated sharing of data by tackling both technical obstacles, as well as systematic obstacles to interoperability, such as information blocking.

At the same time, we believe that ONC’s approach to defining information blocking is complex and confusing. As a result, well-intentioned physicians may be inappropriately implicated simply due to a lack of clarity regarding their role and responsibilities. Physicians need a clear understanding of when they are obligated to release data and when it is appropriate to hold on to data. ***It is critical that ONC clearly and thoroughly educate physicians and other stakeholders on how to navigate the fine balance between HIPAA, which dictates that physicians not share data unless they have a permissible purpose, and the information blocking rules, which dictates that physicians must share data unless they meet an exception. Furthermore, because of the ongoing lack of clarity regarding the responsibility of the physician vis-à-vis these competing requirements, we strongly recommend that ONC focus first on effective education rather than effective deterrents or disincentives.***

## Definitions

### *EHI*

“EHI” is not specifically defined in the Cures Act, HITECH Act, or other relevant statutes. ONC proposes to define “EHI” as:

- ePHI; and
- Any other information that is:
  - Transmitted by or maintained in electronic media, as defined in 45 CFR § 160.103;
  - Identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual; and
  - 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.

This proposed definition of EHI is expansive and could include information on an individual’s health insurance eligibility and benefits, billings for health care services, and payment information for services

to be provided or already provided, which may include price information. However, ONC clarifies that EHI would not include health information that is de-identified in accordance with HIPAA.

***The Alliance believes that this definition is too broad and subjective for the purposes of enforcing information blocking. We recommend that the information blocking provisions only apply to the data classes in the USCDI, which aligns with the API certification requirements proposed in this rule.*** HHS notes throughout the ONC and CMS rules that the USCDI is well-positioned to facilitate care coordination and to promote interoperability.

#### *Health Care Providers, Health IT Developers, Exchanges, and Networks*

ONC proposes to adopt a definition of “actors” that is consistent with the four classes of individuals and entities mentioned in the Cures Act: 1) health care providers; 2) developers of certified HIT; 3) health information networks (HINs); and 4) health information exchanges (HIEs). According to ONC, the defining attribute of a “HIN” is that it enables, facilitates, or controls the movement of information between or among different individuals or entities that are unaffiliated. “HIE” is more narrowly defined as an individual or entity that enables access, exchange, or use of EHI primarily between or among a particular class of individuals or entities or for a limited set of purposes. ONC cites a clinical data registry as an example of an HIE, since it might facilitate or enable the access, exchange, or use of EHI for a limited scope of participants and purposes.

The Alliance is concerned that the broad definitions of both “HIE” and “HIN” could implicate registries and other innovative data collection platforms in regards to the data blocking restrictions. Clinical data registries are used to monitor aggregate trends for quality improvement, patient safety, and/or research purposes—they are not intended to focus on the individual patient. Oftentimes, the registry is not even the originating source of the data. Furthermore, registry data is often de-identified and cannot easily be linked back to an individual. As noted earlier, ONC clarifies in this section of the rule that EHI would not include health information that is de-identified in accordance with HIPAA. ***Thus, the Alliance believes that it is unreasonable to include registries in the list of actors that would be regulated by the information blocking provisions and to hold registries accountable for ensuring that patient-specific data is easily and regularly accessible to the patient or a third-party requestor.***

We also request clarification on whether health plans would be included under the list of “actors” subject to the information blocking provisions. Although they are not specifically identified, would they fall under the definition of HIE or HIN? ***It is important that health plans are included on the list of regulated actors since health plans manage huge amounts of data on individual patients and would be required, under the CMS rule, to share such data with patients and providers.***

#### Practices Likely to Interfere with Access, Exchange, or Use of EHI

ONC provides a list of activities that would likely interfere with access, exchange, or use of EHI. Because information blocking may take many forms, ONC notes it is not possible to anticipate or catalog the many potential types of practices that may raise information blocking concerns and that it will examine actions on a case-by-case basis. The Alliance appreciates ONC’s attempt to not be overly prescriptive with its definition of information blocking. At the same time, this leaves physicians without clear direction as to the actions they need to take to ensure they are not accused of information blocking. Rather than flesh out an explicit definition of information blocking, ONC characterizes it based almost entirely on proposed *exceptions* to rules. This strategy results in ambiguous parameters for a complex

issue. ***We strongly urge ONC to provide physicians with more clarity on information blocking, including guidance documents with additional specific examples of what does constitute information blocking and clear instructions on steps physicians can take to avoid being accused of it. It is also important for ONC to provide assurances that if a physician tries, in good faith, to comply with an exception or otherwise not engage in information blocking, and has done his/her due diligence and documents it, that ONC would strongly consider such evidence in assessing an allegation of information blocking. Finally, we request that ONC consider protections for small practices and solo practitioners who may be at increased risk of information blocking simply because they do not have the resources or technical infrastructure that larger providers may have to ensure compliance.***

#### Proposed Exceptions to Information Blocking

ONC proposes seven exceptions to the general prohibition on information blocking, some of which are discussed below. We remind ONC that there is still a considerable amount of grey area in terms of what would qualify as an “exception” and what would not. ***We recommend that ONC provide clearer, more comprehensive guidance regarding what activities would qualify for each of these exceptions and exactly what physicians would have to do to document compliance and avoid being accused of information blocking. It also is critical that ONC adopt clear and consistent criteria for evaluating information blocking complaints and require that actors disclose the methodologies behind their fees or otherwise provide clear documentation to defend their actions during an information blocking investigation. In carrying out these policies, ONC should aim to find a balance between ensuring the legitimacy of exception claims and minimizing any documentation burden to actors.***

#### *Promoting the Privacy of EHI/Promoting the Security of EHI*

The Alliance is concerned that the “Promoting the Privacy of EHI” and “Promoting the Security of EHI” exceptions may be used inappropriately (or even innocently) by actors who may refuse to share data based on the false premise that such transfer of data somehow violates HIPAA. As we noted earlier, the proposals in this rule represent a major paradigm shift in regards to a physician’s responsibilities over patient data. Under HIPAA, which this rule does nothing to change, physicians are instructed to exercise caution in regards to the release of data whereas now, under the information blocking provisions, a physician may be obligated to release such data. Physicians will find it extremely challenging to navigate these conflicting mandates. ***At least initially, it is critical that HHS focus its efforts on educating physicians on their obligations under HIPAA and these new information blocking provisions rather than penalizing them for infractions.***

#### *Recovering Costs Reasonably Incurred*

Under this proposed exception, it will not be information blocking for an actor to recover its reasonable costs of enabling access, exchange, or use of EHI. To date, unreasonably high fees charged by EHR vendors have been one of the principle impediments to the seamless, electronic exchange of health information. The Alliance is concerned that EHR vendors will use this exception to justify charging physicians inappropriately high fees to cover the cost of complying with all the new requirements in this rule. ***It is critical that ONC adopt an objective and verifiable process to specifically evaluate whether the fees that actors are charging are truly reasonable and are being applied fairly and uniformly across similar stakeholders.*** As discussed earlier, API Data Providers (i.e., “physicians”) will be responsible for covering all of these fees since they are limited in their ability to recoup such costs from patients.

### *Responding to Requests that are Infeasible*

Again, the Alliance is concerned that EHR vendors will inappropriately use this exception to justify denying access to data. ***We support ONC's proposal that in the event that an actor determines that providing EHI in a particular manner is not feasible, it must provide the requestor with a detailed written explanation of the reasons why the actor cannot accommodate the request and it must work with the requestor in a timely manner to provide a reasonable alternative means of accessing, exchanging, or using the EHI.***

### *Licensing of Interoperability on Reasonable and Non-Discriminatory Terms*

This proposed exception to the information blocking provision would permit actors to license interoperability elements on reasonable and non-discriminatory. The license can impose a reasonable royalty, but must include appropriate rights so that the licensee can develop, market, and/or enable the use of interoperable products and service.

To date, EHR vendor efforts to protect intellectual property via licensing have interfered considerably with interoperability. Oftentimes, these vendors will even consider their source data proprietary and will not allow third parties to access it without their permission, even though it is primarily patient data. As such, we appreciate that ONC acknowledges in this section that EHR vendors use licensing agreements to control source code and data. ***Given this ongoing and serious issue, we request that ONC tighten this exception to: 1) clarify that the actual data within software should never be licensed; and 2) to prevent EHR vendors from charging unreasonably high fees through the use of royalties when licensing interoperability elements.***

### **RFI on Price Transparency and Information Blocking**

Through subsequent rulemaking, ONC hopes to expand access to price information for the public, prospective patients, plan sponsors, and health care providers, and includes a series of questions on how best to do this. Some of the specific topics on which ONC seeks feedback include:

- The potential parameters and implications of including price information in the definition of EHI for purposes of information blocking;
- Whether it should require health IT developers to include in their platforms a mechanism for patients and providers to have access to price information through APIs;
- Whether price information should be made available on public web sites so that patients can shop for care without having to contact individual providers, and if so, who should be responsible for posting such information.

As discussed throughout this comment letter, the Alliance supports efforts to enhance patient access to healthcare data, but we are skeptical of the utility of such information if it is provided out of context, in a non-consumer friendly format, or in such a large volume that it overwhelms patients. Price data, alone, does not tell the whole story of patient care options and will be of little significance to patients if not presented in the context of quality and against the backdrop of longer-term value. In specialty medicine, in particular, the price tag for a single procedure may be much higher than a single primary care visit, but the procedure may be the more cost-effective option for the patient over the long-run. Furthermore, because of our nation's complex coding and billing system, what appears as a single condition or service may be captured through multiple codes so it is not so simple to translate service charges into an easily digestible format.

***As HHS continues to contemplate ways to enhance price transparency, it needs to be mindful of the unique nuances that factor into healthcare decision-making and to work to ensure that patients understand their full range of options and the potential implications of each of those options. Furthermore, we believe that payers— not hospitals or physicians— should be responsible for releasing price information and presenting it in a way that is useful for the patient.*** Providers are already crushed with administrative tasks that interfere with their clinical responsibilities; the proposals in this rule will only add to that burden. Providers also have very little direct influence over healthcare prices other than charge rates. For example, a surgeon cannot predict a patient’s out-of-pocket costs on the day of surgery since these costs may change between the patient’s initial visit and the day of the procedure. It is also important to keep in mind that small practices have very little negotiating power with payers. While larger health systems may have more control over prices, practices with less resources and clout have little ability to influence rates and simply take the rate that payers dictate. On the other hand, payers maintain control over negotiated rates, have full access to (and control of) patient cost-sharing information, and know details such as how much of a deductible a patient has already paid. The Alliance strongly believes that payers, and not providers, should be responsible for making price information available to patients. Putting this burden on providers would further interfere with patient care as providers would have to spend time tracking down this information from payers.

***Finally, we urge HHS to start small and to proceed gradually when rolling out any future price transparency initiatives.*** For example, HHS should first carefully test the feasibility and utility of making limited price data available, such as formulary driven prescription prices or elective procedures, which are more predictable and easier to capture.

## **Registries RFI**

Section 4005 (a) and (b) of the Cures Act focuses on interoperability and bidirectional exchange between EHRs and registries, including clinician-led clinical data registries. 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. Many clinicians continue to rely on manual entry when submitting data to specialty-sponsored registries since their EHRs will not accommodate direct transmission of data. This is unfortunate since it requires costly workarounds and generally stymies efforts to comprehensively track, evaluate, and improve quality of care. ***The Alliance believes that ONC’s proposed standards for certified APIs, as well as its proposed restrictions on information blocking, have the potential to improve how information is exchanged with registries. We also believe they will promote a more systematic collection of standardized clinical and other health data.***

## **RFI on Policies to Improve Patient Matching**

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

The Alliance agrees that patient matching is a critical issue. Although the process of linking the correct

medical record to the correct patient seems like a basic task, it is one at which systems, even when made by the same EHR vendor, often fail. Inaccurate patient matching can lead to adverse events, compromised safety and privacy, inappropriate and unnecessary care, unnecessary burden on both patients and providers, increased health care costs, and poor oversight of fraud and abuse. Furthermore, in the absence of mechanisms, such as a Unique Patient Identifier (UPI), to ensure that relevant records are all tied to the same patient, safe and secure electronic exchange of health information is constrained. ***The Alliance appreciates that both CMS and ONC are looking into alternative solutions to this ongoing problem. While we do not have a specific recommendation, we urge both agencies to evaluate potential solutions, such as patient matching algorithms, carefully to ensure they do not exacerbate current challenges and lead to more errors or increased administrative burden.***

### **Conclusion**

The Alliance thanks ONC for the opportunity to share our feedback on these ground-breaking proposals. As we mentioned up front, if HHS' goal is to make patients better healthcare consumers and to provide clinicians with easier access to information that will lead to more appropriate and efficient care, then it is critical for ONC to carry out these reforms carefully and gradually. If the infrastructure is not first in place to minimize potential risks, then this initiative will backfire in ways that could lead to greater confusion and impact coverage, access to care, and quality of care. The proposals in this rule represent a major paradigm shift with major implications, but also hold great potential if carried out appropriately.

The Alliance looks forward to working with ONC as it embarks down this path. Should you have any questions, please contact us at [info@specialtydocs.org](mailto:info@specialtydocs.org).

Sincerely,

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