AMERICAN ACADEMY OF FAMILY PHYSICIANS

June 3, 2019

Alex M. Azar II, Secretary
Department of Health and Human Services
Office of the National Coordinator for Health Information Technology
Mary E. Switzer Building
Mail Stop: 7033A
330 C Street SW
Washington, DC 20201

Dear Secretary Azar:

On behalf of the American Academy of Family Physicians (AAFP), which represents 134,600 family physicians and medical students across the country, I write in response to the proposed rule titled, "21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program" as published by the Office of the Secretary in the March 4, 2019, *Federal Register*.

The AAFP applauds the Administration's continued push toward a nationwide interoperable health care system. Family physicians routinely struggle with acquiring the right health information to make the best decisions with their patients. The lack of interoperability is a fundamental issue leading to increased cost, burden, and frustration as well as lowering quality and health.

The *21st Century Cures Act* is a welcome new component of our national health policy and makes information blocking illegal. The challenge HHS must overcome is to thread the needle between penalizing true information blockers while not adding complexity, uncertainty, and burden upon practices who are not blocking information.

When reviewing each individual portion, such as an exception, the AAFP believes the proposed provisions around information blocking form an appropriate framework. However, we harbor significant concerns that in total the framework adds unnecessary complexity and uncertainty for our members.

We strongly encourage HHS to work aggressively to simplify the rules with small- and medium-sized physician practices in mind. Furthermore, HHS should create more certainty through safe harbors for small practices that are acting in good faith to be interoperable. The AAFP urges HHS to provide specific clarity regarding the conflict between the "minimum necessary" information sharing language in the *Health Insurance Portability and Accountability Act* (HIPAA) and the "maximum available information" sharing described in this proposed rule.

A key area that HHS should simplify and clarify is the definition of Electronic Health Information (EHI). As currently proposed, the definition is unclear and could be too expansive. We recommend that HHS define EHI rather as two sets of data. Set one are those data that are part of the United States Core Data for Interoperability (USCDI). Set two are those data that (1) are reasonability requested and (2) are reasonably available for exchange. Set one is a well-defined, standards-based data set whereas set two is not. Given that certified EHR technology is tested to support USCDI, these data should be reasonability available for exchange. Set two data could be burdensome to make available for exchange or may not even be available, such as claims data from a practice. Information blocking should only be implicated when EHI is requested but not exchanged if it was reasonably available for exchange. Without the stipulation whether EHI is "requested," we are concerned that compliance departments within health care organizations will default to send all data for every exchange. Unintended consequences such as this interpretation have occurred with the transitions of care exchange requirements of Meaningful Use. Given that certified EHR technology is not guaranteed to be able to semantically process all incoming data, the end-user (i.e. the physician) is required to review all the data to extract critical clinical information. This adds significant burden on physicians if large volumes of clinically irrelevant data is included in the exchange.

Regarding Certification of EHR Technology, the AAFP strongly encourages HHS to focus solely on interoperability and patient safety concerns. Doing so would limit the unintended consequences of the proposed rule such as poor workflows and increased costs, which occurred as part of certification for Meaningful Use. We urge HHS to make the interoperability criteria very robust and for ONC-Authorized Certification Bodies to perform rigorous testing, including real-world testing in deployed systems.

The AAFP strongly supports the move toward open Application Programming Interfaces (APIs) and standards-based APIs. However, when APIs are combined with Information Blocking and HIPAA regulations we are concerned that managing complex sharing permissions and consents will be too taxing on small- and medium-sized physician practices. The 2015 Edition CEHRT, as proposed in this rule, does not have criteria for functionality that supports practices and physicians to collect, store, and enforce complex sharing authorizations via APIs and other means. The AAFP is concerned that a significant increase in administrative burdens on practices will occur if the regulation is implemented as currently proposed. We strongly recommend that HHS create a temporary exception to information blocking until the standards for Data Segmentation for Privacy have matured and have been properly implemented in CEHRT.

The AAFP urges HHS to keep current administrative burdens on practices top of mind in regard to the choice of enforcement regime to deter information blocking These burdens hobble practices' ability to comply with current paperwork requirements, and compliance with information blocking protocols can not add to this burden. In addition, the proposed rule states that one instance of information blocking can qualify as a violation. The AAFP believes that a lone violation should not result in a penalty, especially for small- and medium-sized practices; rather, information blocking should require a pattern of behavior. Additionally, the proposed rule does not establish a process or framework for how HHS will evaluate whether a violation has occurred, and an appropriate penalty for the violation. We strongly encourage HHS to propose and receive public comment on a framework for the process of auditing a practice to unearth evidence of a violation. That audit process should require HHS to have the burden of proof to show evidence of information blocking rather than proof that no information blocking occurred. The AAFP strongly recommends HHS phase in penalties for information blocking through the

implementation of a temporary safe harbor for a consecutive 24-month period after the rule is in effect.

Reducing the cost of interoperability is strongly supported by the AAFP. We are pleased to see the proposed rule limits fees by vendors to those that are "necessary and reasonable," yet the AAFP is concerned that EHR Vendors, App developers, Payers, and Health Information Exchanges can charge necessary and reasonable fees, yet physicians and practices are precluded from charging patients such necessary and reasonable fees. As proposed by the rule, physicians would be left with the cost of interoperability without an ability to recoup those expenses. **The AAFP strongly recommends HHS either allow all entities to charge necessary and reasonable expenses or bar all entities from charging for interoperability costs**. Of course, not allowing necessary and reasonable fees would stifle innovation and development toward interoperability.

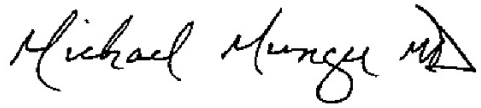
Lastly, we are concerned with the timelines laid out in the proposed rule. HHS should avoid the experience of Meaningful Use which included repeatedly adjusted timelines. Instead the timelines should provide ample space to implement the needed functionalities and workflows and provide a consistent, predicable series of deadlines. Therefore, we ask HHS to relax the timelines as laid out in the proposed rule.

Given the impact and complexity of this proposed rule, we request that HHS release a Supplemental Notice of Proposed Rulemaking with comment period rather than a Final Rule.

The AAFP offers additional comments and recommendations within the template provided to improve the proposed rule.

We appreciate the opportunity to provide these comments. Please contact Steven E. Waldren, MD, MS, Vice President and Chief Medical Informatics Officer, at 913-906-6165 or swaldren@aafp.org with any questions or concerns.

Sincerely,



Michael L. Munger, MD, FAAFP
Board Chair

About Family Medicine
Family physicians conduct approximately one in five of the total medical office visits in the United States per year—more than any other specialty. Family physicians provide comprehensive, evidence-based, and cost-effective care dedicated to improving the health of patients, families, and communities. Family medicine's cornerstone is an ongoing and personal patient-physician relationship where the family physician serves as the hub of each patient's integrated care team. More Americans depend on family physicians than on any other medical specialty.

21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program

Section III – Deregulatory Actions for Previous Rulemakings

Removal of Randomized Surveillance Requirements
We propose to revise § 170.556(c) by changing the requirement that ONC-Authorized Certification Bodies (ONC-ACBs) must conduct in-the-field, randomized surveillance to specify that ONC-ACBs may conduct in-the-field, randomized surveillance. We further propose to remove the following: • The specification that ONC-ACBs must conduct randomized surveillance for a minimum of 2% of certified health IT products per year. • Requirements regarding the exclusion and exhaustion of selected locations for randomized surveillance. • Requirements regarding the consecutive selection of certified health IT for randomized surveillance. Without these regulatory requirements, ONC-ACBs would still be required to perform reactive surveillance, and would be permitted to conduct randomized surveillance of their own accord, using the methodology identified by ONC with respect to scope and selection method, and the number and types of locations for in-the-field surveillance.
Preamble FR Citation: 84 FR 7434 **Specific questions in preamble?** *No*
Regulatory Impact Analysis: Please see 84 FR 7562-63 for estimates related to the removal of randomized surveillance requirements.
Public Comment Field: The AAFP is very supportive of real-world testing of CEHRT. This is an essential component of an effective CEHRT oversight framework.

Removal of the 2014 Edition from the Code of Federal Regulations
We propose to remove the 2014 Edition certification criteria (§ 170.314) and related standards, terms, and requirements from the rule.
Preamble FR Citation: 84 FR 7434-35 **Specific questions in preamble?** *No*
Regulatory Impact Analysis: Please see 84 FR 7563-64 for estimates related to the removal of the 2014 Edition from the Code of Federal Regulations.
Public Comment Field: The AAFP supports this removal for two key reasons: (1) it further simplifies certification for physicians as 2014 Edition is no longer relevant and (2) the AAFP believes that certification should be focused solely on interoperability and patient safety issues.

Removal of Certain 2015 Edition Certification Criteria
We propose to remove certain certification criteria, including criteria that are and are not currently included in the 2015 Edition Base EHR definition at §170.102. We propose to remove from § 170.315 and § 170.102 the following 2015 Edition Criteria that are currently included in the 2015 Edition Base EHR definition: • "problem list" • "medication list" • "medication allergy list" • "drug formulary and preferred drug list checks" • "smoking status" We also propose to remove from § 170.315 the following 2015 Edition certification criteria that are not included in the 2015 Edition Base EHR definition: • Patient-specific education resources • Common Clinical Data Set Summary (CCDS) Record – Create • Common Clinical Data Set Summary (CCDS) Record – Receive • Secure Messaging
Preamble FR Citation: 84 FR 7435-37 **Specific questions in preamble?** *No*
Regulatory Impact Analysis: Please see 84 FR 7565-66 for estimates related to the removal of certain 2015 Edition certification criteria and standards.

Public Comment Field:

The AAFP supports this removal for two key reasons: (1) it further simplifies certification for physicians as 2014 Edition is no longer relevant and (2) the AAFP believes that certification should be focused solely on interoperability and patient safety issues.

Request for Information on the Development of Similar Independent Program Processes

Recognition of the FDA Software Pre-Certification Program for purposes of certification of health IT to 2015 Edition criteria may eventually be determined to be infeasible or insufficient to meet our goals of reducing burden and promoting innovation. With this in mind, we request comment on whether ONC should establish new regulatory processes tailored towards recognizing the unique characteristics of health IT (e.g., electronic health record (EHR) software) by looking first at the health IT developer, rather than primarily at the health IT presented for certification, as is currently done under the Program. We also welcome more specific comments on the health IT developer criteria for such an approach and what the Conditions and/or Maintenance of Certification requirements should be to support such an approach within the framework of the proposed Conditions and Maintenance of Certification requirements discussed in section VII of this proposed rule.

Preamble FR Citation: 84 FR 7439 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

The AAFP believes that certification of products should be focused solely on interoperability and patient safety issues. The AAFP believes that certification of developers and/or their processes would be an appropriate area for ONC. For example, ensuring the developer is following best practices in user-centered design would be appropriate.

Section IV – Updates to the 2015 Edition Certification Criteria

§ 170.213 United States Core Data for Interoperability (USCDI)

We propose to adopt the USCDI at new § 170.213: "Standard. United States Core Data for Interoperability (USCDI), Version 1 (v1) (incorporated by reference in § 170.299)."

We propose to revise the following 2015 Edition certification criteria to incorporate the USCDI standard in place of the "Common Clinical Data Set" (currently defined at § 170.102 and proposed for removal in this rule):

- ''Transitions of care'' (§ 170.315(b)(1));
- ''view, download, and transmit to 3rd party'' (§ 170.315(e)(1));
- ''consolidated CDA creation performance'' (§ 170.315(g)(6));
- ''transmission to public health agencies—electronic case reporting'' (§ 170.315(f)(5)); and
- ''application access—all data request'' (§ 170.315(g)(9)).]

Preamble FR Citation: 84 FR 7441 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Please see 84 FR 7567-68 for estimates related to this proposal.

Public Comment Field:

The AAFP supports the adoption of the USCDI as a standard and as a replacement for the CCDS. We agree that predicable, transparent, collaborative, and ***agile*** processes are needed to accelerate the expansion of the USCDI. The AAFP has joined other organizations in the HSPC/CIIC effort to establish semantic data models to support interoperability and sharing of knowledge. The AAFP looks forward to bringing clinician-led, consensus-driven data standards to ONC for incorporation into future versions of the USCDI.

Unique Device Identifier (UDI) for a Patient's Implantable Devices: CDA Implementation Guide

The recently published Health Level 7 (HL7®) CDA R2 Implementation Guide: C-CDA Supplemental Templates for Unique Device Identification (UDI) for Implantable Medical Devices, Release 1-US Realm identifies changes needed to the C-CDA to better facilitate the exchange of the individual UDI components in the health care system when devices are implanted in a patient. We request comment on whether we should add this recently published UDI IG as a requirement for health IT in order to meet the requirements for UDI USCDI Data Class. In addition, we do not have a reliable basis on which to estimate how much it would cost to meet the requirements outlined in the UDI IG; and, therefore, we request comment on the cost and burden of complying with this proposed requirement.

Preamble FR Citation: 84 FR 7443 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Not Applicable

Public Comment Field:

The AAFP is concerned about increasing the cost of ambulatory EHRs due to this certification requirement. The AAFP recommends that this ***not*** be included in 2015 Edition CEHRT. Rather, this could be included in a voluntary specialty/domain specific future certification.

Medication Data Request for Comment

The USCDI v1 "Medication" data class includes two constituent data elements within it: Medications and Medication Allergies. With respect to the latter, Medication Allergies, we request comment on an alternative approach. This alternative would result in removing the Medication Allergies data element from the Medication data class and creating a new data class titled, "Substance Reactions," which would be meant to be inclusive of "Medication Allergies." The new "Substance Reactions" data class would include the following data elements: "Substance" and "Reaction," and include SNOMED CT as an

Preamble FR Citation: 84 FR 7443 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Not Applicable

Public Comment Field:

Clinically, as long as the data is able to be queried and physicians can see a list of Medication Allergies, the representation is less important. While it makes sense from an informatics standpoint, the new data class should be "Adverse Reactions" as there are adverse reactions that may not be substance related but still clinically useful.

§ 170.315(b)(10) Electronic health information export
Included in 2015 Edition Base EHR Definition? *Yes*
Electronic health information export. (i) Single patient electronic health information export. (A) Enable a user to timely create an export file(s) with all of a single patient's electronic health information the health IT produces and electronically manages on that patient. (B) A user must be able to execute this capability at any time the user chooses and without subsequent developer assistance to operate. (C) Limit the ability of users who can create such export file(s) in at least one of these two ways: (1) To a specific set of identified users. (2) As a system administrative function. (D) The export file(s) created must be electronic and in a computable format. (E) The export file(s) format, including its structure and syntax, must be included with the exported file(s). (ii) Database export. Create an export of all the electronic health information the health IT produces and electronically manages. (A) The export created must be electronic and in a computable format. (B) The export's format, including its structure and syntax must be included with the export. (iii) Documentation. The export format(s) used to support single patient electronic health information export as specified in paragraph (b)(10)(i) of this section and database export as specified in paragraph (b)(10)(ii) of this section must be made available via a publicly accessible hyperlink.
Preamble FR Citation: 84 FR 7446-49 **Specific questions in preamble?** *Yes*
Regulatory Impact Analysis: Please see 84 FR 7568-70 for estimates related to this proposal.
Public Comment Field: Family physicians experience high costs to extract data on patient populations out of EHRs or have been told to manually extract each patient in the EHR user interface. The AAFP strongly supports the inclusion of database export as a criterion for 2015 Edition CEHRT.

§ 170.315(b)(12) Data segmentation for privacy – send
Included in 2015 Edition Base EHR Definition? *No*
Data segmentation for privacy – send. Enable a user to create a summary record formatted in accordance with the standard adopted in § 170.205(a)(4) and (a)(4)(i) that is tagged as restricted at the document, section, and entry (data element) level and subject to restrictions on re-disclosure according to the standard adopted in § 170.205(o)(1).
Preamble FR Citation: 84 FR 7452 **Specific questions in preamble?** *Yes*
Regulatory Impact Analysis: Please see 84 FR 7575-77 for estimates related to this proposal.
Public Comment Field: The data segmentation for privacy criteria do not provide sufficient functionality to support physicians to collect, store, and enforce complex sharing authorizations via APIs and other means. The AAFP is concerned that the certification for data segmentation and the information blocking provisions of the proposed rule will significantly increase administrative burdens on family physicians. The certification criteria for data segmentation should be more robust. ONC should initiate an exception to the information blocking provisions that protects practices that do not share information due to the lack of capability in their CEHRT to manage complex sharing permissions.

§ 170.315(b)(13) Data segmentation for privacy – receive
Included in 2015 Edition Base EHR Definition? *No*
Data segmentation for privacy – receive. Enable a user to: (i) Receive a summary record that is formatted in accordance with the standard adopted in § 170.205(a)(4) and (a)(4)(i) that is tagged as restricted at the document, section, and entry (data element) level and subject to restrictions on re-disclosure according to the standard adopted in § 170.205(o)(1); and (ii) Preserve privacy markings to ensure fidelity to the tagging based on consent and with respect to sharing and re-disclosure restrictions.
Preamble FR Citation: 84 FR 7452 **Specific questions in preamble?** *Yes*
Regulatory Impact Analysis: Please see 84 FR 7575-77 for estimates related to this proposal.

Public Comment Field:

The data segmentation for privacy criteria do not provide sufficient functionality to support physicians to collect, store, and enforce complex sharing authorizations via APIs and other means. The AAFP is concerned that the certification for data segmentation and the information blocking provisions of the proposed rule will significantly increase administrative burdens on family physicians. The certification criteria for data segmentation should be more robust. ONC should initiate an exception to the information blocking provisions that protects practices that do not share information due to the lack of capability in their CEHRT to manage complex sharing permissions.

Section V – Modifications to the ONC Health IT Certification Program

§ 170.550 Health IT Module certification

* * * * *

(e) ONC-ACBs must provide an option for certification of Health IT Modules to any one or more of the criteria referenced in § 170.405(a) based on newer versions of standards included in the criteria which have been approved by the National Coordinator for use in certification through the Standards Version Advancement Process.

(f) [Reserved]

(g) * * *

(5) Section 170.315(b)(10) when the health IT developer of the health IT presented for certification produces and electronically manages electronic health information.

(h) * * *

(3) * * *

(i) Section 170.315(a)(1), (2), (3), (5) through (8), (11), and (12) are also certified to the certification criteria specified in § 170.315(d)(1) through (7). Section 170.315(a)(4), (9), (10), and (13) are also certified to the certification criteria specified in § 170.315(d)(1), (2), (3), (5), (6), and (7).

* * * * *

(iii) Section 170.315(c) is also certified to the certification criteria specified in § 170.315(d)(1), (2)(i)(A), (B), (ii) through (v), (3), and (5);

* * * * *

(v) Section 170.315(e)(2) and (3) is also certified to the certification criteria specified in § 170.315(d)(1), (d)(2)(i)(A), (B), (ii) through (v), (3), (5), and (9);

* * * * *

(vii) Section 170.315(g)(7) through (11) is also certified to the certification criteria specified in § 170.315(d)(1) and (9); and (d)(2)(i)(A), (2)(i)(B), 2(ii) through (v), or (10);

(viii) Section 170.315(h) is also certified to the certification criteria specified in § 170.315(d)(1), (2)(i)(A), (2)(i)(B), (2)(ii) through (v), and (3); and

* * * * *

(ix) If applicable, any criterion adopted in § 170.315 is also certified to the certification criteria specified in § 170.315(d)(12) and/or (13).

* * * * *

(l) Conditions of Certification Attestations. Before issuing a certification, ensure that the health IT developer of the Health IT Module has met its responsibilities under subpart D of this part.

Preamble FR Citation: 84 FR 7454-55 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Please see 84 FR 7559 and 84 FR 7582-83 for estimates related to this proposal.

§ 170.550 Health IT Module certification

Public Comment Field:

The AAFP continues to support modular certification.

Section VI – Health IT for the Care Continuum

Approach to Health IT for the Care Continuum and the Health Care of Children

Section 4001(b)(i) of the Cures Act instructs the National Coordinator to encourage, keep, or recognize, through existing authorities, the voluntary certification of health IT under the Program for use in medical specialties and sites of service for which no such technology is available or where more technological advancement or integration is needed. This provision of the Cures Act closely aligns with ONC's ongoing collaborative efforts with both federal partners and stakeholders within the health care and health IT community to encourage and support the advancement of health IT for a wide range of clinical settings. Section VI of this proposed rule outlines our approach to implement Section 4001(b) of the Cures Act, which requires that the Secretary make recommendations for the voluntary certification of health IT for use by pediatric health providers and to adopt certification criteria to support the voluntary certification of health IT for use by pediatric health providers to support the health care of children. To be clear, and consistent with past practice, we do not recommend or propose a "pediatric-specific track or program" under the ONC Health IT Certification Program. This proposed rule outlines the certification criteria adopted in the 2015 Edition which we believe support the certification of health IT for pediatric care.

Preamble FR Citation: 84 FR 7457-61 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

The AAFP is supportive of a voluntary process for certification. This allows for the non-voluntary certification process to be focused on interoperability and patient safety. The AAFP is supportive of the development of a pediatric specific voluntary certification.

Request for Information on Health IT and Opioid Use Disorder Prevention and Treatment

We seek comment in this proposed rule on a series of questions related to health IT functionalities and standards to support the effective prevention and treatment of opioid use disorder (OUD) across patient populations and care settings. Specifically, we request public comment on how our existing Program requirements (including the 2015 Edition certification criteria) and the proposals in this rulemaking may support use cases related to OUD prevention and treatment and if there are additional areas that ONC should consider for effective implementation of health IT to help address OUD prevention and treatment. This section also includes request for comment on furthering adoption and use of electronic prescribing of controlled substances standard and neonatal abstinence syndrome.

Preamble FR Citation: 84 FR 7461-65	**Specific questions in preamble?** *Yes*
Regulatory Impact Analysis: Not applicable	
Public Comment Field: The AAFP strongly encourages HHS to harmonize e-prescribing and Prescription Drug Monitoring Programs (PDMP). The same standards to exchange information about controlled substances should be used. Supporting a separate PDMP exchange infrastructure within practices when an established and robust e-prescribing infrastructure is in place is wasteful. Physicians and other clinicians should be able to seamlessly access controlled drug fulfillment and prescribing history from within their EHR aggregated across multiple states.	

Section VII – Conditions and Maintenance of Certification

Note: Because this template presents comment tables in the order in which their subject proposed provisions are discussed in the preamble of the proposed rule, this section includes tables for certain new and revised provisions in 45 CFR subparts A, B, C, and E, in complement to the proposed new subpart D.

§ 170.401 Information blocking Condition and Maintenance of Certification Requirement
(a) Condition of Certification. A health IT developer must not take any action that constitutes information blocking as defined in 42 U.S.C. 300jj-52 and § 171.103. (b) Maintenance of Certification. [Reserved]
Preamble FR Citation: 84 FR 7465 **Specific questions in preamble?** *No*
Regulatory Impact Analysis: Not applicable
Public Comment Field: The AAFP supports judicious use of Conditions and Maintenance of Certification, such that there are limited mandates for all stakeholders to participate in HHS programs. Conditions laid out in the NPRM are judicious and the AAFP is supportive. However, the AAFP has concerns about the timeline laid out in the NPRM of 24 months since some developers may not be able to meet that deadline; and therefore, their clients would be unable to participate in HHS programs. The AAFP asks for provisions in the final rule that would hold clients of such developers harmless for 12 months (i.e. those clients could still participate in the Quality Payment Program (QPP) with decreases in their score on Promoting Interoperability) from the date of the completion of the change.

§ 170.403 Communications

(a) Condition of Certification.

(1) A health IT developer may not prohibit or restrict the communication regarding—

(i) The usability of its health IT;

(ii) The interoperability of its health IT;

(iii) The security of its health IT;

(iv) Relevant information regarding users' experiences when using its health IT;

(v) The business practices of developers of health IT related to exchanging electronic health information; and

(vi) The manner in which a user of the health IT has used such technology.

(2) A health IT developer must not engage in any practice that prohibits or restricts a communication regarding the subject matters enumerated in paragraph (a)(1) of this section, unless the practice is specifically permitted by this paragraph and complies with all applicable requirements of this paragraph.

(i) Unqualified protection for certain communications. A health IT developer must not prohibit or restrict any person or entity from communicating any information or materials whatsoever (including proprietary information, confidential information, and intellectual property) when the communication is about one or more of the subject matters enumerated in paragraph (a)(1) of this section and is made for any of the following purposes—

(A) Making a disclosure required by law;

(B) Communicating information about adverse events, hazards, and other unsafe conditions to government agencies, health care accreditation organizations, and patient safety organizations;

(C) Communicating information about cybersecurity threats and incidents to government agencies;

(D) Communicating information about information blocking and other unlawful practices to government agencies; or

(E) Communicating information about a health IT developer's failure to comply with a Condition of Certification, or with any other requirement of this part, to ONC or an ONC-ACB.

(ii) Permitted prohibitions and restrictions. For communications about one or more of the subject matters enumerated in paragraph (a)(1) of this section that is not entitled to unqualified protection under paragraph (a)(2)(i) of this section, a health IT developer may prohibit or restrict communications only as expressly permitted by paragraphs (a)(2)(ii)(A) through (F) of this section.

(A) Developer employees and contractors. A health IT developer may prohibit or restrict the communications of the developer's employees or contractors.

(B) Non-user-facing aspects of health IT. A health IT developer may prohibit or restrict communications that disclose information about non-user-facing aspects of the developer's health IT.

(C) Intellectual property. A health IT developer may prohibit or restrict communications that would infringe the intellectual property rights existing in the developer's health IT (including third-party rights), provided that—

(1) A health IT developer does not prohibit or restrict, or purport to prohibit or restrict, communications that would be a fair use of a copyright work; and

(2) A health IT developer does not prohibit the communication of screenshots of the developer's health IT, subject to the limited restrictions described in paragraph (a)(2)(ii)(D) of this section.

(D) Screenshots. A health IT developer may require persons who communicate screenshots to—

(1) Not alter screenshots, except to annotate the screenshot, resize it, or to redact the screenshot in accordance with § 170.403(a)(2)(ii)(D)(3) or to conceal protected health information;

(2) Not infringe the intellectual property rights of any third parties, provided that—

(i) The developer has used all reasonable endeavors to secure a license (including the right to sublicense) in respect to the use of the third-party rights by communicators for purposes of the communications protected by this Condition of Certification;

(ii) The developer does not prohibit or restrict, or purport to prohibit or restrict, communications that would be a fair use of a copyright work;

(iii) The developer has put all potential communicators on sufficient written notice of each aspect of its screen display that contains third-party content that cannot be communicated because the reproduction would infringe the third-party's intellectual property rights; and

(iv) Communicators are permitted to communicate screenshots that have been redacted to not disclose third-party content; and

§ 170.403 Communications

(3) Redact protected health information, unless the individual has provided all necessary consents or authorizations or the communicator is otherwise authorized, permitted, or required by law to disclose the protected health information.

(E) Pre-market testing and development. A health IT developer may prohibit or restrict communications that disclose information or knowledge solely acquired in the course of participating in pre-market product development and testing activities carried out for the benefit of the developer or for the joint benefit of the developer and communicator. A developer must not, once the subject health IT is released or marketed for purposes other than product development and testing, and subject to the permitted prohibitions and restrictions described in paragraph (a)(2)(ii) of this section, prohibit or restrict communications about matters enumerated in paragraph (a)(1) of this section.

(b) Maintenance of Certification.

(1) Notice. Health IT developers must issue a written notice to all customers and those with which it has agreements containing provisions that contravene paragraph (a) of this section:

(i) Within six months of the effective date of the final rule that any communication or contract provision that contravenes paragraph (a) of this section will not be enforced by the health IT developer.

(ii) Within one year of the final rule, and annually thereafter until paragraph (b)(2)(ii) of this section is fulfilled, that any communication or contract provision that contravenes paragraph (a) of this section will not be enforced by the health IT developer.

(2) Contracts and agreements.

(i) A health IT developer must not establish or enforce any contract or agreement that contravenes paragraph (a) of this section.

(ii) If a health IT developer has a contract or agreement in existence at the time of the effective date of this final rule that contravenes paragraph (a) of this section, then the developer must in a reasonable period of time, but not later than two years from the effective date of this rule, amend the contract or agreement to remove or void the contractual provision that contravenes paragraph (a) of this section.

Preamble FR Citation: 84 FR 7467-76 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Please see 84 FR 7578 for estimates related to this proposal.

Public Comment Field:

The AAFP strongly supports these requirements on health IT developers.

VII.B.4 Real World Testing

§ 170.405 Real world testing

(a) Condition of Certification. A health IT developer with Health IT Modules to be certified to any one or more 2015 Edition certification criteria in § 170.315(b), (c)(1) through (3), (e)(1), (f), (g)(7) through (11), and (h) must successfully test the real world use of those Health IT Module(s) for interoperability (as defined in 42 U.S.C.300jj(9) and § 170.102) in the type of setting in which such Health IT Module(s) would be/is marketed.

(b) Maintenance of Certification.

(1) Real world testing plan submission. A health IT developer must submit an annual real world testing plan to its ONC-ACB via a publicly accessible hyperlink no later than December 15 of each calendar year for each of its certified 2015 Edition Health IT Modules that include certification criteria referenced in paragraph (a) of this section.

(i) The plan must be approved by a health IT developer authorized representative capable of binding the health IT developer for execution of the plan and include the representative's contact information.

(ii) The plan must include all health IT certified to the 2015 Edition through August 31st of the preceding year.

(ii) The plan must address the following for each of the certification criteria identified in paragraph (a) of this section that are included in the Health IT Module's scope of certification:

(A) The testing method(s)/methodology(ies) that will be used to demonstrate real world interoperability and conformance to the certification criteria's requirements, including scenario- and use case-focused testing;

(B) The care setting(s) that will be tested for real world interoperability and an explanation for the health IT developer's choice of care setting(s) to test;

(C) The timeline and plans for any voluntary updates to standards and implementation specifications that the National Coordinator has approved through the Standards Version Advancement Process.

(D) A schedule of key real world testing milestones;

(E) A description of the expected outcomes of real world testing;

(F) At least one measurement/metric associated with the real world testing; and

(G) A justification for the health IT developer's real world testing approach.

(2) Real world testing results reporting. A health IT developer must submit real world testing results to its ONC-ACB via a publicly accessible hyperlink no later than January 31 each calendar year for each of its certified 2015 Edition Health IT Modules that include certification criteria referenced in paragraph (a) of this section. The real world testing results must report the following for each of the certification criteria identified in paragraph (a)of this section that are included in the Health IT Module's scope of certification:

(i) The method(s) that was used to demonstrate real world interoperability;

(ii) The care setting(s) that was tested for real world interoperability;

(iii) The voluntary updates to standards and implementation specifications that the National Coordinator has approved through the Standards Version Advancement Process.

§ 170.405 Real world testing

(iv) A list of the key milestones met during real world testing;

(v) The outcomes of real world testing including a description of any challenges encountered during real world testing; and

(vi) At least one measurement/metric associated with the real world testing.

(3) USCDI Updates for C-CDA. A health IT developer with health IT certified to § 170.315(b)(1), (e)(1), (g)(6), (f)(5), and/or (g)(9) prior to the effective date of this final rule must:

(i) Update their certified health IT to be compliant with the revised versions of these criteria adopted in this final rule; and

(ii) Provide its customers of the previously certified health IT with certified health IT that meets paragraph (b)(3)(i) of this section within 24 months of the effective date of this final rule.

(4) C-CDA Companion Guide Updates. A health IT developer with health IT certified to § 170.315(b)(1), (b)(2), (b)(9), (e)(1), (g)(6), and/or (g)(9) prior to the effective date of this final rule must:

(i) Update their certified health IT to be compliant with the revised versions of these criteria adopted in this final rule; and

(ii) Provide its customers of the previously certified health IT with certified health IT that meets paragraph (b)(4)(i) of this section within 24 months of the effective date of this final rule.

(5) Voluntary standards and implementation specifications updates. A health IT developer subject to paragraph (a) of this section that voluntary updates its certified health IT to a new version of an adopted standard that is approved by the National Coordinator through the Standards Version Advancement Process must:

(i) Provide advance notice to all affected customers and its ONC-ACB –

(A) Expressing its intent to update the software to the more advanced version of the standard approved by the National Coordinator;

(B) The developer's expectations for how the update will affect interoperability of the affected Health IT Module as it is used in the real world;

(C) Whether the developer intends to continue to support the certificate for the existing certified Health IT Module version for some period of time and how long or if the existing certified Health IT Module version will be deprecated; and

(ii) Successfully demonstrate conformance with approved more recent versions of the standard(s) or implementation specification(s) included in applicable 2015 Edition certification criterion specified in

Preamble FR Citation: 84 FR 7495-97 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Please see 84 FR 7578-82 for estimates related to this proposal.

Public Comment Field:

The AAFP is a strong supporter of real-world testing. There are significant factors in implementation that can impact the EHR that would not be tested in the lab.

VII.D Enforcement

§ 170.581 Certification ban

(a) Circumstances trigger a certification ban. The certification of any of a health IT developer's health IT is prohibited when:

(1) The certification of one or more of the health IT developer's Complete EHRs or Health IT Modules is:

(i) Terminated by ONC under the ONC Health IT Certification Program;

(ii) Withdrawn from the ONC Health IT Certification Program by an ONC-ACB because the health IT developer requested it to be withdrawn when the health IT developer's health IT was the subject of a potential non-conformity or non-conformity as determined by ONC;

(iii) Withdrawn by an ONC-ACB because of a non-conformity with any of the certification criteria adopted by the Secretary under subpart C of this part;

(iv) Withdrawn by an ONC-ACB because the health IT developer requested it to be withdrawn when the health IT developer's health IT was the subject of surveillance for a certification criterion or criteria adopted by the Secretary under subpart C of this part, including notice of pending surveillance; or

(2) ONC determines a certification ban is appropriate per its review under § 170.580(a)(2)(iii).

(b) Notice of certification ban. When ONC decides to issue a certification ban to a health IT developer, ONC will notify the health IT developer of the certification ban through a notice of certification ban. The notice of certification ban will include, but may not be limited to:

§ 170.581 Certification ban

(1) An explanation of the certification ban;

(2) Information supporting the certification ban;

(3) Instructions for appealing the certification ban if banned in accordance with paragraph (a)(2) of this section; and

(4) Instructions for requesting reinstatement into the ONC Health IT Certification Program, which would lift the certification ban.

(c) Effective date of certification ban.

(1) A certification ban will be effective immediately if banned under paragraphs (a)(1) of this section.

(2) For certification bans issued under paragraph (a)(2) of this section, the ban will be effective immediately after the following applicable occurrence:

(i) The expiration of the 10-day period for filing a statement of intent to appeal in § 170.580(g)(3)(i) if the health IT developer does not file a statement of intent to appeal.

(ii) The expiration of the 30-day period for filing an appeal in § 170.580(g)(3)(ii) if the health IT developer files a statement of intent to appeal, but does not file a timely appeal.

(iii) A final determination to issue a certification ban per § 170.580(g)(7) if a health IT developer files an appeal timely.

(d) Reinstatement. The certification of a health IT developer's health IT subject to the prohibition in paragraph (a) of this section may commence once the following conditions are met.

(1) A health IT developer must request ONC's permission in writing to participate in the ONC Health IT Certification Program.

(2) The request must demonstrate that the customers affected by the certificate termination, certificate withdrawal, or non-compliance with a Condition or Maintenance of Certification have been provided appropriate remediation.

(3) For non-compliance with a Condition or Maintenance of Certification requirement, the non-compliance must be resolved.

(4) ONC is satisfied with the health IT developer's demonstration under paragraph (d)(2) of this section that all affected customers have been provided with appropriate remediation and grants reinstatement into the ONC Health IT Certification Program.

Preamble FR Citation: 84 FR 7504-06 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

EHR clients whose developer has been banned should be afforded a 24-month safe harbor from any HHS penalties (i.e. QPP) by HHS. This would give the practice an opportunity to migrate to another CEHRT.

Section VIII – Information Blocking

§ 171.103 Information blocking

Information blocking means a practice that—

(a) Except as required by law or covered by an exception set forth in subpart B of this part, is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information; and

(b) If conducted by a health information technology developer, health information exchange, or health information network, such developer, exchange, or network knows, or should know, that such practice is likely to interfere with, prevent, or materially discourage the access, exchange, or use of electronic health information; or

(c) If conducted by a health care provider, such provider knows that such practice is unreasonable and is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information.

Preamble FR Citation: 84 FR 7508 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Please see 84 FR 7584-86 for estimates related to this proposal.

Public Comment Field:

The AAFP agrees with the inclusion of "that such practice is unreasonable" in the definition covering health care providers. The AAFP believes that health care providers that are acting in good faith should not be considered information blocking. Because HHS chose to use the good faith standard as part of the definition, there will be a dramatical reduction in the complexity and uncertainty for practices and physicians to comply with the proposed rule. This good faith requirement must also be central in the audit process for the implementation of the rule.

§ 171.102 Definitions

Exchange means the ability for electronic health information to be transmitted securely and efficiently between and among different technologies, systems, platforms, or networks in a manner that allows the information to be accessed and used.Fee means any present or future obligation to pay money or provide any other thing of value.

Health care provider has the same meaning as ‘‘health care provider’’ at 42 U.S.C. 300jj.

Health Information Exchange or HIE means an individual or entity that enables access, exchange, or use of electronic health information primarily between or among a particular class of individuals or entities or for a limited set of purposes.

Health Information Network or HIN means an individual or entity that satisfies one or both of the following—

(1) Determines, oversees, administers, controls, or substantially influences policies or agreements that define business, operational, technical, or other conditions or requirements for enabling or facilitating access, exchange, or use of electronic health information between or among two or more unaffiliated individuals or entities.

(2) Provides, manages, controls, or substantially influences any technology or service that enables or facilitates the access, exchange, or use of electronic health information between or among two or more unaffiliated individuals or entities.

Health IT developer of certified health IT means an individual or entity that develops or offers health information technology (as that term is defined in 42 U.S.C. 300jj(5)) and which had, at the time it engaged in a practice that is the subject of an information blocking claim, health information technology (one or more) certified under the ONC Health IT Certification Program.

Information blocking is defined as it is in § 171.103 and 42 U.S.C. 300jj-52(a).

Interfere with means to prevent, materially discourage, or otherwise inhibit access, exchange, or use of electronic health information.

Interoperability element means—

(1) Any functional element of a health information technology, whether hardware or software, that could be used to access, exchange, or use electronic health information for any purpose, including information transmitted by or maintained in disparate media, information systems, health information exchanges, or health information networks.

(2) Any technical information that describes the functional elements of technology (such as a standard, specification, protocol, data model, or schema) and that a person of ordinary skill in the art may require to use the functional elements of the technology, including for the purpose of developing compatible technologies that incorporate or use the functional elements.

(3) Any technology or service that may be required to enable the use of a compatible technology in production environments, including but not limited to any system resource, technical infrastructure, or health information exchange or health information network element.

(4) Any license, right, or privilege that may be required to commercially offer and distribute compatible technologies and make them available for use in production environments.

§ 171.102 Definitions

(5) Any other means by which electronic health information may be accessed, exchanged, or used.

Permissible purpose means a purpose for which a person is authorized, permitted, or required to access, exchange, or use electronic health information under applicable law.

Person is defined as it is in 45 CFR 160.103.

Protected health information is defined as it is in 45 CFR 160.103.

Practice means one or more related acts or omissions by an actor.

Use means the ability of health IT or a user of health IT to access relevant electronic health information; to comprehend the structure, content, and meaning of the information; and to read, write, modify, manipulate, or apply the information to accomplish a desired outcome or to achieve a desired purpose.

Preamble FR Citation: 84 FR 7509-15 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

Electronic Health Information (EHI)

As currently proposed, the definition is unclear and could be too expansive. The AAFP recommends that HHS define EHI rather as two sets of data. Set one are those data that are part of the United States Core Data for Interoperability (USCDI). Set two are those data that (1) are reasonably requested and (2) are reasonably available for exchange. Set one is a well-defined, standards-based data set, whereas set two is not. Given that certified EHR technology is tested to support USCDI, these data should be reasonably available for exchange. Set two data could be burdensome to make available for exchange or may not even be available, such as claims data from a practice. Information blocking should only be implicated when EHI is requested but not exchanged if it was reasonably available for exchange. By breaking EHI into these two data sets, HHS could develop different policies for each data set as it relates to timeliness of exchange needed, use of APIs for exchange, etc. The AAFP believes reasonableness should be part of the EHI definition and not just an exception to the information blocking provision.

Missing Definition: Health IT developer of NON-certified Health IT

Not all health IT in the ecosystem is or will become certified EHR technology. The role of such developers and applications in the proposed rule is unclear. The AAFP believes that this class of developer/application needs to be explicitly defined and referenced throughout the proposed rule.

Request for comment regarding the definition of "health care provider"

The term "health care provider" is defined in Public Health Service Act section 3000(3) (42 U.S.C. 300jj(3)). We propose to adopt this definition for purposes of section 3022 of the PHSA when defining "health care provider" in § 171.102. We note that this definition is different from the definition of "health care provider" under the HIPAA Privacy and Security Rules. We are considering adjusting the information blocking definition of "health care provider" to cover all individuals and entities covered by the HIPAA "health care provider" definition. We seek comment on whether this approach would be justified, and commenters are encouraged to specify reasons why doing so might be necessary to ensure that the information blocking provision applies to all health care providers that might engage in information blocking.

Preamble FR Citation: 84 FR 7510 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

The AAFP recommends that the definition from HIPAA be used for "health care provider."

Request for comment regarding price information (ONC)

We seek comment on the parameters and implications of including price information within the scope of EHI for purposes of information blocking.

Preamble FR Citation: 84 FR 7513-14 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

Price transparency is critically important for value-based care. The AAFP supports the inclusion of pricing data in the definition of EHI. However, the AAFP has a major concern about the availability of such data. This is a prime example of why the AAFP recommends that the definition of EHI be revised to include only data that is reasonably available for exchange. With the AAFP's revised definition of EHI, we would support the inclusion of pricing data in the definition of EHI (Set two per AAFP's proposed definition).

Request for comment regarding price information (Department of Health and Human Services)

The overall Department seeks comment on the technical, operational, legal, cultural, environmental and other challenges to creating price transparency within health care.

Preamble FR Citation: 84 FR 7513-14 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

The AAFP believes that transparency in health care refers to reporting information which can be easily verified for accuracy. Both data and process should have transparency and an explicit disclosure of data limitations. With this in mind, a major challenge to price transparency within health care is the ease of verification of accuracy, because even if "prices" are posted in a transparent manner, there is no easy way to verify their accuracy as far as the patient is concerned, since the "sticker price" is often not what the patient or other consumer must pay due to negotiated write-offs, rebates, etc. These limitations or qualifications to posted "prices" are typically not disclosed in an explicit manner, further challenging the realization of price transparency.

Of course, to accommodate all the limitations and qualifications attendant to health care "prices" may present technical, operational, and other challenges that make it nearly impossible to be transparent about "prices" in a cost-effective manner. Concurrently, these challenges raise fundamental questions about the definition of "price" in this context.

Existing anti-trust laws may also pose legal challenges to achieving universal price transparency. For instance, it is less than clear whether providers of health care are protected from charges of collusion or price fixing if they make their prices known in a transparent way.

Beyond these issues, there appear to be no cultural or environmental challenges to price transparency in health care. Americans are used to researching the price of almost anything online in the 21st century and equally comfortable sharing information on almost anything via social media. As Americans, we are transparent in almost all other aspects of our lives, and we know of no cultural or environmental reasons Americans would be challenged by price transparency in health care.

Request for comment regarding practices that may implicate the information blocking provision

We request comment regarding our proposals about practices that may implicate the information blocking provision. Specifically, we seek comment on:

- Our proposed approach regarding observational health information and encourage commenters to identify potential practices related to non-observational health information that could raise information blocking concerns.
- The circumstances described and other circumstances that may present an especially high likelihood that a practice will interfere with access, exchange, or use of EHI within the meaning of the information blocking provision.

Preamble FR Citation: 84 FR 7515-21 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

The AAFP supports the distinction between observational health information and non-observational health information. We agree that lack of access or exchange of many non-observational health information should not implicate the information blocking provision. The AAFP has concern about the proposed rule's statement, *"...practices that adversely impact the access, exchange, or use of observational health information will almost always implicate the information blocking provision."* The term "almost always" is too much of a universal qualifier. Not all observational health information will have significant clinical value in the future and therefore it may not be retained. For example, continuous vital sign monitoring has limited value after a specific health encounter and produces a large burden to collect and retain, although the health IT system may store the waveform data for a short period of time. Should a practice of deleting that observational data after the encounter implicate the information blocking provision? The AAFP believes not. Observational data with a reasonable clinical future use might implicate the information blocking provision.

§ 171.200 Availability and effect of exceptions

A practice shall not be treated as information blocking if the actor satisfies an exception to the information blocking provision by meeting all applicable requirements and conditions of the exception at all relevant times.

Preamble FR Citation: 84 FR 7522 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

When reviewing each individual portion, such as an exception, the AAFP believes the proposed rule lays out an appropriate framework. However, we harbor significant concerns that in total the framework adds unnecessary complexity and uncertainty for our members. It is unclear what process HHS will use to evaluate an implication of the information blocking provision and apply the exceptions. The rigor of the documentation needed by the health care provider to justify their restriction on access, exchange, or use of EHI is unclear. Health care providers are also burdened with trying to comply with conflicting state and federal laws. **Although the information blocking framework is exception based, we strongly believe that the burden should lay with HHS to prove information blocking occurred rather than the health care provider to prove that it did not.**

The AAFP strongly encourages HHS in the final rule to work aggressively to simplify the rules with small- and medium-sized physician practices in mind. Furthermore, HHS should create more certainty through safe harbors for small practices that are acting in good faith to be interoperable. The AAFP urges HHS to provide specific clarity regarding the conflict between the "minimum necessary" information sharing language in the *Health Insurance Portability and Accountability Act* (HIPAA) and the "maximum available information" sharing described in this proposed rule.

VIII.D Proposed Exceptions to the Information Blocking Provision

§ 171.202 Exception – Promoting the privacy of electronic health information

provide access, exchange, or use of electronic health information provided that the actor's practice—

(1) Complies with applicable state or federal privacy laws;

(2) Implements a process that is described in the actor's organizational privacy policy;

(3) Had previously been meaningfully disclosed to the persons and entities that use the actor's product or service;

(4) Is tailored to the specific privacy risk or interest being addressed; and

(5) Is implemented in a consistent and non-discriminatory manner.

(d) Denial of an individual's request for their electronic protected health information in the circumstances provided in 45 CFR 164.524(a)(1), (2), and (3). If an individual requests their electronic protected health information under 45 CFR 164.502(a)(1)(i) or 45 CFR 164.524, the actor may deny the request in the circumstances provided in 45 CFR 164.524(a)(1), (2), or (3).

(e) Respecting an individual's request not to share information. In circumstances where not required or prohibited by law, an actor may choose not to provide access, exchange, or use of an individual's electronic health information if—

(1) The individual requests that the actor not provide such access, exchange, or use;

(2) Such request is initiated by the individual without any improper encouragement or inducement by the actor;

(3) The actor or its agent documents the request within a reasonable time period; and

(4) The actor's practice is implemented in a consistent and non-discriminatory manner.

Preamble FR Citation: 84 FR 7526-35 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

Maintaining the trust of patients is critical to good patient care and therefore, the AAFP is strongly supportive of exceptions to promote patient privacy. We also believe health care provider privacy is important to maintain. The AAFP has deep concern that this exception will add significant burden to health care providers in that they must be the arbiters between state and federal (and among federal) laws. HHS needs to do the work and pre-arbitrate the conflicts between privacy laws/rules and provide the health care provider with clear guidance on how the collections of laws should be interpreted and what should be the appropriate actions of the health care provider.

§ 171.203 Exception – Promoting the security of electronic health information

To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.

(a) The practice must be directly related to safeguarding the confidentiality, integrity, and availability of electronic health information.

(b) The practice must be tailored to the specific security risk being addressed.

(c) The practice must be implemented in a consistent and non-discriminatory manner.

(d) If the practice implements an organizational security policy, the policy must—

(1) Be in writing;

(2) Have been prepared on the basis of, and directly respond to, security risks identified and assessed by or on behalf of the actor;

(3) Align with one or more applicable consensus-based standards or best practice guidance; and

(4) Provide objective timeframes and other parameters for identifying, responding to, and addressing security incidents.

(e) If the practice does not implement an organizational security policy, the actor must have made a determination in each case, based on the particularized facts and circumstances, that:

(1) The practice is necessary to mitigate the security risk to the electronic health information; and

(2) There are no reasonable and appropriate alternatives to the practice that address the security risk that are less likely to interfere with, prevent, or materially discourage access, exchange or use of electronic health information.

Preamble FR Citation: 84 FR 7535-38 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

Security is critical to protecting patient health information to enable privacy and confidentiality as well as ensure availability of health information. The AAFP strongly supports an exception to promote security of EHI. We have significant concern with ensuring the security of third-party applications as well as ensuring the identity of actors requesting EHI. These requirements will result in significant burdens on health care providers, especially those in small businesses. It is unreasonable to think that a small business health care provider would have the capability or capacity to perform the security vetting of third-party applications to access their CEHRT. These providers will be dependent on external validation and certification. Without this, it is improbable for a small business health care provider to ensure security of EHI if they allow access by those third-party applications. Limiting access to EHI via API due to not being able to evaluate a third-party application's security should not be a violation of the information blocking provision.

§ 171.204 Exception – Recovering costs reasonably incurred

(1) Notwithstanding any other provision of this exception, if the actor is a health IT developer subject to the Conditions of Certification in § 170.402(a)(4) or § 170.404 of this subchapter, the actor must comply with all requirements of such conditions for all practices and at all relevant times.

(2) If the actor is an API Data Provider, the actor is only permitted to charge the same fees that an API Technology Supplier is permitted to charge to recover costs consistent with the permitted fees specified in the Condition of Certification in § 170.404 of this subchapter.

Preamble FR Citation: 84 FR 7538-41 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

We are pleased to see the proposed rule limits fees by vendors to those that are "necessary and reasonable," yet the AAFP is concerned that EHR Vendors, App developers, Payers, and Health Information Exchanges can charge necessary and reasonable fees but physicians may not. As a result, physicians will be left with the bill for interoperability without an ability to recoup those expenses. **The AAFP strongly recommends HHS either allow all entities to charge necessary and reasonable expenses or bar all entities from charging for interoperability costs.**

§ 171.205 Exception – Responding to requests that are infeasible

(viii) The additional cost and burden to the requestor and other relevant persons of relying on alternative means of access, exchange, or use.

(2) The following circumstances do not constitute a burden to the actor for purposes of this exception and shall not be considered in determining whether the actor has demonstrated that complying with a request would have been infeasible.

(i) Providing the requested access, exchange, or use in the manner requested would have facilitated competition with the actor.

(ii) Providing the requested access, exchange, or use in the manner requested would have prevented the actor from charging a fee.

(b) Responding to requests. The actor must timely respond to all requests relating to access, exchange, or use of electronic health information, including but not limited to requests to establish connections and to provide interoperability elements.

(c) Written explanation. The actor must provide the requestor with a detailed written explanation of the reasons why the actor cannot accommodate the request.

(d) Provision of a reasonable alternative. The actor must work with the requestor in a timely manner to identify and provide a reasonable alternative means of accessing, exchanging, or using the electronic health information.

Preamble FR Citation: 84 FR 7542-44 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

The AAFP supports a requirement to document that a request was infeasible, yet we have concern that the documentation requirements outlined in this exception are overly burdensome. This is especially true in that there is no restriction on the requestor to make a reasonable request. A family physician could be inundated with requests that are not reasonable. The AAFP recommends that the documentation requirement for this exception be reduced to (1) a timely response that the request is not feasible with a simple statement with the high-level reason it is infeasible and (2) an example of what would be feasible if an alternative is available.

VIII.F Complaint Process

Information blocking complaint process

ONC requests comment on the current complaint process approach and any alternative approaches that would best effectuate this aspect of the Cures Act. In addition to any other comments that the public may wish to submit, we specifically request comment on a list of specific issues related to the complaint process.

Preamble FR Citation: 84 FR 7552-53 Specific questions in preamble? *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

As the AAFP believes that HHS must prove information blocking instead of a health care provider proving there was *no* information blocking, the reporting of potential information blocking should contain enough detail for HHS to be confident there is willful information blocking to be investigated.

VIII.G Disincentives for Health Care Providers – Request for Information

Request for information on disincentives for health care providers

We request information on disincentives or if modifying disincentives already available under existing HHS programs and regulations would provide for more effective deterrents to information blocking. We also seek information on the implementation of section 3022(d)(4) of the PHSA, which provides that in carrying out section 3022(d) of the PHSA, the Secretary shall, to the extent possible, not duplicate penalty structures that would otherwise apply with respect to information blocking and the type of individual or entity involved as of the day before December 13, 2016 – enactment of the Cures Act.

Preamble FR Citation: 84 FR 7553 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

In regard to an enforcement regime to deter information blocking, the AAFP urges HHS to keep current administrative burdens on physician practices top of mind. These burdens hobble practices' ability to comply with current paperwork requirements, and compliance with information blocking protocols must not add to this burden. In regard to specific policies, the proposed rule states that one instance of information blocking can qualify as a violation. The AAFP believes that a lone violation should not result in a penalty, especially for small- and medium-sized practices; rather, Information Blocking should require a pattern of behavior. Additionally, the proposed rule does not establish a process or framework for how HHS will evaluate whether a violation has occurred. Nor is an appropriate penalty for the violation proposed. **We strongly encourage HHS to propose and receive public comments on a framework for the process of auditing a practice to unearth evidence of a violation. That audit process should require HHS to carry the burden of proof to show evidence of information blocking rather than the practice being required to prove that there was *not* information blocking. Finally, the AAFP strongly recommends HHS phase in the penalties for information blocking through the implementation of a temporary safe harbor for a consecutive 24-month period after the rule is in effect.**

Health care providers should not be subject duplicative disincentives. Health care providers already will see disincentives under the Quality Payment Program, which requires attestation that the health care provider is not engaging in information blocking. Therefore, those health care providers participating in the QPP should not receive additional disincentives under the information blocking provision as they would be duplicative.