Consumer Technology Association™

1919 S. Eads St.
Arlington, VA 22202
703-907-7600
CTA.tech

June 3, 2019

Don Rucker, M.D.
Office of the National Coordinator for Health Information Technology (ONC)
U.S. Department of Health and Human Services
330 C St SW
Floor 7
Washington, DC 20201

BY ELECTRONIC SUBMISSION

Re: Consumer Technology Association Public Comments in Response to Request for Comments on the Proposed 21st Century Cures Act Rule

Dear Dr. Rucker:

The Consumer Technology Association (CTA™) appreciates the opportunity to submit comments in response to the Office of the National Coordinator for Health Information Technology's (ONC) 21st Century Cures Act proposed rule, published in the Federal Register on March 4, 2019. As detailed in the following comments and Appendix A, CTA supports ONC's efforts to improve sharing of electronic health information and patient access and has provided comments to further these goals.

About CTA

CTA is the trade association representing the $398 billion U.S. consumer technology industry, which supports more than 15 million U.S. jobs. More than 2,200 companies—80 percent are small businesses and startups; others are among the world's best-known brands—enjoy the benefits of CTA membership including policy advocacy, market research, technical education, industry promotion, standards development and the fostering of business and strategic relationships. CTA also owns and produces CES® – the world's gathering place for all who thrive on the business of consumer technologies. Profits from CES are reinvested into CTA's industry services.

The Health Information Technology for Economic and Clinical Health (HITECH) Act started the nation on a path towards realizing the benefits of electronic health information, but unreasonable information blocking and poor consumer access to their health information has left much of the benefits

of electronic health information unfulfilled. CTA believes that consumer technology can facilitate substantial improvements in the delivery of health care, but only if consumers have the ability to readily obtain their electronic health information in a usable electronic format and if unreasonable information blocking is prohibited.

General Comments

The following are general comments to the proposed rule. We then follow these general comments with more specific suggestions using the ONC comment template.

Updates to the 2015 Edition Certification Criteria. CTA supports ONC's decision to modify the 2015 Edition, rather than creating an entirely new edition of certification criteria for certified electronic health record technology (CEHRT). We believe this more incremental approach best serves the health care provider and health IT developer community at this time. Similarly, CTA supports ONC's proposal to replace the Common Clinical Data Set (CCDS) with the United States Core Data for Interoperability (USCDI), including the flexibility for expansion without the need for full notice-and-comment rulemaking. Finally, CTA supports ONC's efforts to encourage persistent access to all of a patient's electronic health information, the protection of such information through multifactor authentication and encryption, and the use of the Fast Healthcare Interoperability Resources (FHIR) Release 4, and certification criteria for data segmentation at the data entry level and consent management through application program interfaces (API).

Conditions and Maintenance of Certification. CTA supports ONC's efforts to deter and stop information blocking, including the requirement that certain health IT developers participate in the Trusted Exchange Framework and a Common Agreement (TEFCA), the curbing of limitations on communications, flexibility in certification to promote innovation-driven CEHRT, and requiring attestations that developers are complying with their commitment to transparency.

APIs. CTA fully supports the proposed expansion of the use of APIs and increased standardization. CTA believes that increased availability and standardization of APIs will enable patients to receive greater access to their electronic health information through the technology of their choice—allowing for greater patient engagement and care coordination. Specifically, CTA supports the use of FHIR Release 4 (with a sunset provision for future adoption of suitable formats), write-access through APIs, and the adoption of API Resource Collection in Health (ARCH) as the implementation standard.

Automated De-Identification. Although not mentioned in the proposed rules, CTA recommends that ONC consider amending the 2015 Certification Criteria to provide for automated de-identification of electronic health information. While the greater exchange of identifiable electronic health information will substantially improve direct patient care, CTA believes that the increased creation and exchange of de-identified electronic health information is the key to transformative improvements in the health care system at large. Technologies such as machine learning and artificial intelligence can support improvements to treatment protocols that will provide better outcomes at lower costs. While ONC has not requested comments in this area, CTA recommends that ONC consider the following further amendments to the 2015 Edition.

> *De-Identified Information to the Health Care Provider.* CTA recommends that ONC amend the certification criteria to require that CEHRT include functionality that allows a health care

provider to readily create a de-identified data set for all or some of its patient population from structured data using the HIPAA "Safe Harbor" method of de-identification (in which 18 categories of identifiers are removed). This will make it easier for health care providers to generate and share population-level de-identified data with other covered entities and business associates that can be used to improve health care operations and conduct research with minimal risk to the privacy of individuals. We recognize that automated de-identification of unstructured data, such as clinical notes, is far more challenging, and, therefore, believe it should be encouraged but not required. ONC also can encourage health care providers to place contractual restrictions on re-identification of the de-identified data, and CTA supports efforts to legislatively prohibit re-identification without the authorization of the source of the data or the patient.

De-Identified Information to the Patient through an API. While consumers will be able to obtain identifiable electronic health information through an API, CTA recommends that ONC amend the certification criteria to require that CEHRT also include an API function where a patient can obtain de-identified health information about himself or herself. The API would provide access to a de-identified version of all structured data within the individual's record. We recommend that it also provide the patient with the ability to receive unstructured data as part of the de-identified data set, such as the clinical notes, with the warning that unstructured data should be reviewed and could potentially include identifiers. The patient then can share this de-identified data with third parties and even choose to sell this de-identified data. Once again, CTA encourages efforts to legislatively prohibit re-identification without the authorization of the source of the data (the patient in this case) so that the patient can share the de-identified data without concern that the information subsequently will be re-identified.

Deregulatory Actions. CTA commends ONC on its efforts to reduce regulatory burden by removing regulatory obligations whose time has passed or which have proven to be unnecessarily burdensome.

Other Items:

- CTA proposes, as detailed in Appendix A, that the rules further clarify the definitions of "health information exchange" and "health information network" so as to limit their application to unintended entities that are not primarily focused on health information.

- The definition of electronic health information should incorporate price information as such data is crucial to informed decision making by health care patients.

- CTA generally supports the exceptions to information blocking as reasonable and well-balanced.

- Patient matching is an important factor to delivery of accurate and appropriate health care services. CTA supports ONC's exploration of new technology to ensure reliable patient matching.

* * * * *

CTA has provided additional comments on the specific sections that are relevant to its members in the attached Appendix using the ONC public comment template. We thank ONC for the opportunity to comment and welcome the opportunity to discuss these issues in more depth. If you have any questions, please do not hesitate to contact us.

Respectfully submitted,

Consumer Technology Association

Michael Petricone
Senior Vice President, Government and Regulatory Affairs

René Quashie
Vice President, Policy and Regulatory Affairs, Digital Health

Kinsey Fabrizio
Vice President, Member Engagement, Health and Fitness Technology

1919 South Eads St.
Arlington, VA 22202

Appendix A
CTA's Section-By-Section Comments Using ONC Public Comment Template

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: CTA supports ONC's proposal to authorize, rather than require, randomized surveillance. We believe that providing ONC-ACBs with this greater discretion will allow them to better focus their resources, and will reduce the burden on health care providers who (through no fault of their own) are selected to have their CEHRT tested, without materially impacting the oversight of health IT developer's compliance with certification requirements.

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:
CTA supports ONC's removal of the 2014 Edition from the regulations at § 170.314 (the 2011 Edition was previously removed), which will substantially streamline the regulations.

Removal of the ONC-Approved Accreditor from the Program

We propose to remove the ONC-Approved Accreditor (ONC-AA) from the Program, including definitions, processes, and references to ONC-AA throughout the rule. This proposal also includes removing the final rule titled "Permanent Certification Program for Health Information Technology; Revisions to ONC-Approved Accreditor Processes" (76 FR 72636). Because this prior final rule relates solely to the role and removal of the ONC-AA, we propose removing § 170.575, which codified the final rule in the CFR.

Preamble FR Citation: 84 FR 7435 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Please see 85 FR 7564-65 for estimates related to this proposal.

Public Comment Field:
CTA agrees with ONC's decision to end the ONC-Approved Accreditor program and for ONC to solely oversee ONC-ACBs itself. We believe the extra layer of accreditation by the ONC-Approved Accreditors was overly burdensome.

Recognition of Food and Drug Administration Processes

We propose to establish processes that would provide health IT developers that can document successful certification under the Food and Drug Administration (FDA) Software Pre-Certification Pilot Program with exemptions to the ONC Health IT Certification Programs requirements for testing and certification of its health IT to the 2015 Edition "quality management systems" criterion and the 2015 Edition "safety-enhanced design" criterion, as these criteria are applicable to the health IT developer's health IT presented for certification. We also believe that such a "recognition" could be applicable to the functionally-based 2015 Edition ''clinical'' certification criteria.

Preamble FR Citation: 84 FR 7438-39 **Specific questions in preamble?** *No*

Regulatory Impact Analysis: Not Applicable

Public Comment Field:
CTA supports ONC's proposed exemption for health IT developers from certain criteria if they hold precertification under the FDA's Digital Health Software Precertification Program. We believe that this would reduce unnecessary duplication.

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: CTA supports ONC's proposal to move the focus towards a greater emphasis on the health IT developer, rather than each individual piece of software, so that proven health IT developers with a record of meeting appropriate standards can obtain certification of new EHR technology more quickly. We believe that such a program should be complementary to, rather than in lieu of, the FDA Digital Health Software Precertification Program, so that we do not lose the benefit of FDA's experience in regulating entities in the area of safety and efficacy.

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: CTA supports ONC's proposal to replace the Common Clinical Data Set (CDS) with the more robust and flexible USCDI in § 170.213. The USCDI includes additional data elements, such as clinical notes and data provenance (potentially identifying when and who created particular data), which will be of great value to patients and consumer technology companies that seek to appropriately leverage health data for the patient's benefit. Additionally, CTA supports ONC's proposal to allow for more flexibility in expanding the USCDI without going through full notice-and-comment rulemaking. We believe that this move will lead to great availability of robust health data for appropriate purposes. We would, however, like to see additional specificity and clarity on the relationship between the data that patients are required to be able to access and the USCDI.

§ 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: CTA supports ONC's proposal to require CEHRT to make all of a patient's electronic health information available for export. Further, CTA believes that providing patients and technology companies acting on their behalf persistent access to all electronic health information, rather than a limited set of data, will lead to significantly improved patient engagement and care coordination. Accordingly, CTA supports ONC's effort to move towards persistent access to all electronic health information through APIs and recommends that ONC set forth a specific timeframe for health IT developers to achieve this goal.

§ 170.315(d)(12) Encrypt authentication credentials
Included in 2015 Edition Base EHR Definition? *No*
Encrypt authentication credentials. Health IT developers must assess their Health IT Modules' capabilities and make one of the following attestations: (i) "Yes." Health IT Module encrypts stored authentication credentials in accordance with standards adopted in § 170.210(a)(2). (ii) "No." Health IT Module does not encrypt stored authentication credentials.
Preamble FR Citation: 84 FR 7450 **Specific questions in preamble?** *Yes*
Regulatory Impact Analysis: Please see 84 FR 7575 for estimates related to this proposal.
Public Comment Field: CTA supports ONC's proposal, agreeing that it will promote the best practice of encryption of authentication credentials through increased transparency without significant additional burden on health IT developers.

§ 170.315(d)(13) Multi-factor authentication
Included in 2015 Edition Base EHR Definition? *No*
Multi-factor authentication. Health IT developers must assess their Health IT Modules' capabilities and make one of the following attestations: (i) "Yes." Health IT Module supports authentication through multiple elements the identity of the user with industry recognized standards. (ii) "No." Health IT Module does not support authentication through multiple elements the identity of the user with industry recognized standards.
Preamble FR Citation: 84 FR 7450-51 **Specific questions in preamble?** *Yes*
Regulatory Impact Analysis: Please see 84 FR 7575 for estimates related to this proposal.
Public Comment Field: CTA supports ONC's proposal, agreeing that it will promote the best practice of availability of multi-factor authentication through increased transparency without significant additional burden on health IT developers.

§ 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: CTA supports the increased granularity of tagging at the document, section, or entry level (rather than only the document level), as it supports greater exchange of health information. Specifically, when only a portion of a patient's record is subject to greater confidentiality requirements, this greater level of detail may potentially lead to the exchange of the remainder of the patient's information.

§ 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: CTA supports the increased granularity of tagging at the document, section, or entry level, as it supports greater exchange of health information. Specifically, when only a portion of a patient's record is subject to greater confidentiality requirements, this greater level of detail may potentially lead to the exchange of the remainder of the patient's information.

§ 170.315(g)(11) Consent management for APIs
Included in 2015 Edition Base EHR Definition? *No*
Consent management for APIs. (i) Respond to requests for data in accordance with: (A) The standard adopted in § 170.215(c)(1); and (B) The implementation specification adopted in § 170.215(c)(2). (ii) Documentation. (A) The API(s) must include complete accompanying documentation that contains, at a minimum: (1) API syntax, function names, required and optional parameters supported and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns. (2) The software components and configurations that would be necessary for an application to implement in order to be able to successfully interact with the API and process its response(s). (3) All applicable technical requirements and attributes necessary for an application to be registered with an authorization server. (B) The documentation used to meet paragraph (g)(11)(ii)(A) of this section must be available via a publicly accessible hyperlink.
Preamble FR Citation: 84 FR 7453 **Specific questions in preamble?** *Yes*
Regulatory Impact Analysis: Please see 84 FR 7575 for estimates related to this proposal.
Public Comment Field: CTA supports the addition of certification criteria that supports consent management through APIs in the 2015 Edition, but recommends the use of FHIR Release 4 instead of Release 3 because Release 4 is more stable and has less bugs than Release 3.

Note: Because this template presents comment tables in the order in which the new and revised provisions of 45 CFR parts 170 and 171 are discussed in the preamble of the proposed rule, comment tables for other new and revised certification criteria, standards, and definitions can be found in Section VII, below.

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: CTA supports the Condition of Certification that health IT developers must not take any action that constitutes information blocking. CTA believes that the appropriate flow of electronic health information will lead to significantly improved health care and innovation and agrees that this Condition of Certification supports such efforts.

§ 170.402 Assurances
(a) Condition of Certification. (1) A health IT developer must provide assurances satisfactory to the Secretary that the health IT developer will not take any action that constitutes information blocking as defined in 42 U.S.C. 300jj-52 and § 171.103, unless for legitimate purposes specified by the Secretary; or any other action that may inhibit the appropriate exchange, access, and use of electronic health information. (2) A health IT developer must ensure that its health IT certified under the ONC Health IT Certification Program conforms to the full scope of the certification criteria. (3) A health IT developer must not take any action that could interfere with a user's ability to access or use certified capabilities for any purpose within the scope of the technology's certification. (4) A health IT developer that manages electronic health information must certify health IT to the certification criterion in § 170.315(b)(10). (b) Maintenance of Certification. (1) A health IT developer must retain all records and information necessary to demonstrate initial and ongoing compliance with the requirements of the ONC Health IT Certification Program for: (i) A period of 10 years beginning from the date each of a developer's health IT is first certified under the Program; or (ii) If for a shorter period of time, a period of 3 years from the effective date that removes all of the certification criteria to which the developer's health IT is certified from the Code of Federal Regulations. (2) A health IT developer that must comply with the requirements of paragraph (a)(4) of this section must provide all of its customers of certified health IT with the health IT certified to the certification criterion in § 170.315(b)(10) within 24 months of this final rule's effective date or within 12 months of certification for a health IT developer that never previously certified health IT to the 2015 Edition, whichever is longer.
Preamble FR Citation: 84 FR 7465-66 **Specific questions in preamble?** *Yes*
Regulatory Impact Analysis: Please see 84 FR 7577-78 for estimates related to this proposal.
Public Comment Field: CTA supports the Condition of Certification that health IT developers must commit to not engage in information blocking in the future. CTA believes that the appropriate flow of electronic health information will lead to significantly improved health care and innovation and agrees that this Condition of Certification supports such efforts.

Trusted Exchange Framework and the Common Agreement – Request for Information
We request comment as to whether certain health IT developers should be required to participate in the Trusted Exchange Framework and Common Agreement (TEFCA) as a means of providing assurances to their customers and ONC that they are not taking actions that constitute information blocking or any other action that may inhibit the appropriate exchange, access, and use of EHI. We also welcome comment on the certification criteria we have identified as the basis for health IT developer participation in the Trusted Exchange Framework and adherence to the Common Agreement, other certification criteria that would serve as a basis for health IT developer participation in the Trusted Exchange Framework and adherence to the Common Agreement, and whether the current structure of the Trusted Exchange Framework and Common Agreement are conducive to health IT developer participation and in what manner.
Preamble FR Citation: 84 FR 7466-67 **Specific questions in preamble?** *Yes*
Regulatory Impact Analysis: Not applicable
Public Comment Field: CTA believes that interconnection through the TEFCA will lead to more robust information sharing, with the potential to facilitate consumers receiving access to electronic health information from most or all of their health care providers through a single point. Accordingly, CTA supports requiring health IT developers that provide CEHRT related to health information exchange to provide assurance that they are connected through the TEFCA.

§ 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—

§ 170.403 Communications

(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: CTA supports ONC's proposed Condition of Certification regarding restrictions on communications and agrees that unreasonable contractual restrictions on communications about health IT may impede the continued development and improvement of a more robust health information exchange ecosystem.

VII.B.4 Application Programming Interfaces

§ 170.215(a)(2) API Resource Collection in Health
Implementation specifications. API Resource Collection in Health (ARCH) Version 1.
Preamble FR Citation: 84 FR 7479-80 **Specific questions in preamble?** *Yes*
Regulatory Impact Analysis: Please see 84 FR 7570-75 for estimates related to our proposals regarding APIs.
Public Comment Field: CTA supports ONC's proposal to adopt ARCH Version 1.

§ 170.315(g)(10) Standardized API for patient and population services (Certification Criterion)

Included in 2015 Edition Base EHR Definition? *Yes*

Standardized API for patient and population services. The following technical outcomes and conditions must be met through the demonstration of application programming interface technology.

(i) Data response. Respond to requests for data (based on an ID or other token) for each of the resources referenced by the standard adopted in § 170.215(a)(1) and implementation specifications adopted in § 170.215(a)(2) and (3).

(ii) Search support. Respond to search requests for data consistent with the search criteria included in the implementation specification adopted in § 170.215(a)(4).

(iii) App registration. Enable an application to register with the technology's "authorization server."

(iv) Secure connection. Establish a secure and trusted connection with an application that requests data in accordance with the standard adopted in § 170.215(a)(5).

(v) Authentication and app authorization – 1st time connection. The first time an application connects to request data the technology:

(A) Authentication. Demonstrates that user authentication occurs during the process of authorizing the application to access FHIR resources in accordance with the standard adopted in § 170.215(b).

(B) App authorization. Demonstrates that a user can authorize applications to access a single patient's data as well as multiple patients' data in accordance with the implementation specification adopted in § 170.215(a)(5) and issue a refresh token that is valid for a period of at least 3 months.

(vi) Authentication and app authorization – Subsequent connections. Demonstrates that an application can access a single patient's data as well as multiple patients data in accordance with the implementation specification adopted in § 170.215(a)(5) without requiring re-authorization and re-authentication when a valid refresh token is supplied and issue a new refresh token for new period no shorter than 3 months.

(vii) Documentation.

(A) The API(s) must include complete accompanying documentation that contains, at a minimum:

(1) API syntax, function names, required and optional parameters supported and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns.

(2) The software components and configurations that would be necessary for an application to implement in order to be able to successfully interact with the API and process its response(s).

(3) All applicable technical requirements and attributes necessary for an application to be registered with an authorization server.

(B) The documentation used to meet paragraph (g)(10)(vii)(A) of this section must be available via a publicly accessible hyperlink.

Preamble FR Citation: 84 FR 7481-84 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Please see 84 FR 7570-75 for estimates related to our proposals regarding APIs.

§ 170.315(g)(10) Standardized API for patient and population services (Certification Criterion)

Public Comment Field:

API Standard of FHIR Release 4. ONC identifies four options for what API standard to mandate at § 170.315(g)(10): (1) FHIR Release 2, which 32 percent of health IT developers who have certified to the current API requirements have identified as using; (2) provide health IT developers the option to choose between FHIR Releases 2 and 3; (3) provide health IT developers the option to choose between FHIR Releases 2 and 4; or (4) FHIR Release 4. CTA supports the fourth option, as the industry is currently moving towards Release 4, which is significantly more stable than Releases 2 or 3 due to less software bugs. By the time ONC publishes a final rule and its compliance date arrives, mandating the use of anything less than FHIR Release 4 would constitute a step backgrounds for the health care sector. Accordingly, CTA supports the use of FHIR Release 4 as the standard and believes that health IT developers and app developers will have sufficient time to adopt Release 4 by the compliance date of the future final rule.

Write-Access through APIs. ONC's proposed rule at § 170.315(g)(10) would require APIs that provide third-party apps with read-access to patients' electronic health information, but would not require that APIs include the ability for the apps to write to the electronic health information. ONC states that it "envision[s] a future version of this certification criterion that could include specific 'write' conformance requirements (for example, to aid decision support) once FHIR-based APIs are widely adopted." CTA supports a move towards requiring APIs with both read-access and write-access. This way, patients not only can use apps to download electronic health information from their health care providers' EHRs, but they can also use the apps to upload and share patient-generated health and fitness information with their health care providers in a standard manner. CTA believes that this standardized, bi-directional exchange of information will greatly enhance the opportunity for patient engagement and for health care providers to benefit from the wealth of health and wellness information that consumer technology can generate. CTA recommends that ONC provide a specific timeframe for moving towards requiring APIs to become bi-directional to spur health IT developers to begin to implement API write-access in preparation.

§ 170.404 Application programming interfaces (Condition and Maintenance of Certification)

The following Condition of Certification applies to developers of Health IT Modules certified to any of the certification criteria adopted in § 170.315(g)(7) through (11).

(a) Condition of Certification.

(1) General. An API Technology Supplier must publish APIs and must allow health information from such technology to be accessed, exchanged, and used without special effort through the use of APIs or successor technology or standards, as provided for under applicable law, including providing access to all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws.

(2) Transparency conditions.

(i) General. The business and technical documentation published by an API Technology Supplier must be complete. All documentation published pursuant to paragraph (a)(2)(ii) of this section must be published via a publicly accessible hyperlink that allows any person to directly access the information without any preconditions or additional steps.

(ii) Terms and conditions.

(A) Material information. The API Technology Supplier must publish all terms and conditions for its API technology, including any fees, restrictions, limitations, obligations, registration process requirements, or other similar requirements that would be needed to:

(1) Develop software applications to interact with the API technology;

(2) Distribute, deploy, and enable the use of software applications in production environments that use the API technology;

(3) Use software applications, including to access, exchange, and use electronic health information by means of the API technology;

(4) Use any electronic health information obtained by means of the API technology; and

(5) Register software applications.

(B) API fees. Any and all fees charged by an API Technology Supplier for the use of its API technology must be described in detailed, plain language. The description of the fees must include all material information, including but not limited to:

(1) The persons or classes of persons to whom the fee applies;

(2) The circumstances in which the fee applies; and

§ 170.404 Application programming interfaces (Condition and Maintenance of Certification)

(3) The amount of the fee, which for variable fees must include the specific variable(s) and methodology(ies) that will be used to calculate the fee.

(C) Application developer verification. An API Technology Supplier is permitted to institute a process to verify the authenticity of application developers so long as such process is objective and the same for all application developers and completed within 5 business days of receipt of an application developer's request to register their software application for use with the API Technology Supplier's API technology.

(3) Permitted fees conditions.

(i) General conditions.

(A) All fees related to API technology not otherwise permitted by this section are prohibited from being imposed by an API Technology Supplier.

(B) For all permitted fees, an API Technology Supplier must:

(1) Ensure that fees are based on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests.

(2) Ensure that fees imposed on API Data Providers are reasonably related to the API Technology Supplier's costs of supplying and, if applicable, supporting API technology to, or at the request of, the API Data Provider to whom the fee is charged.

(3) Ensure that the costs of supplying and, if applicable, supporting the API technology upon which the fee is based are reasonably allocated among all customers to whom the API technology is supplied, or for whom the API technology is supported.

(4) Ensure that fees are not based in any part on whether the requestor or other person is a competitor, potential competitor, or will be using the API technology in a way that facilitates competition with the API Technology Supplier.

(ii) Permitted fee – Development, deployment, and upgrades. An API Technology Supplier is permitted to charge fees to an API Data Provider to recover the costs reasonably incurred by the API Technology Supplier to develop, deploy, and upgrade API technology for the API Data Provider.

(iii) Permitted fee – Supporting API uses for purposes other than patient access. An API Technology Supplier is permitted to charge fees to an API Data Provider to recover the incremental costs reasonably incurred by the API Technology Supplier to support the use of API technology deployed by or on behalf of the API Data Provider. This permitted fee does not include:

(A) Any costs incurred by the API Technology Supplier to support uses of the API technology that facilitate a patient's ability to access, exchange, or use their electronic health information;

(B) Costs associated with intangible assets (including depreciation or loss of value), except the actual development or acquisition costs of such assets; or

(C) Opportunity costs, except for the reasonable forward-looking cost of capital.

(iv) Permitted fee – Value-added services. An API Technology Supplier is permitted to charge fees to an API User for value-added services supplied in connection with software that can interact with the API technology, provided that such services are not necessary to efficiently and effectively develop and deploy such software.

§ 170.404 Application programming interfaces (Condition and Maintenance of Certification)

(v) Record-keeping requirements. An API Technology Supplier must keep for inspection detailed records of any fees charged with respect to the API technology, the methodology(ies) used to calculate such fees, and the specific costs to which such fees are attributed.

(4) Openness and pro-competitive conditions. General condition. An API Technology Supplier must grant an API Data Provider the sole authority and autonomy to permit API Users to interact with the API technology deployed by the API Data Provider.

(i) Non-discrimination.

(A) An API Technology Suppler must provide API technology to API Data Providers on terms that are no less favorable than it provides to itself and its own customers, suppliers, partners, and other persons with whom it has a business relationship.

(B) The terms on which an API Technology Supplier provides API technology must be based on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests.

(C) An API Technology Supplier must not offer different terms or service on the basis of:

(1) Whether the API User with whom an API Data Provider has a relationship is a competitor, potential competitor, or will be using electronic health information obtained via the API technology in a way that facilitates competition with the API Technology Supplier.

(2) The revenue or other value the API User with whom an API Data Provider has a relationship may derive from access, exchange, or use of electronic health information obtained by means of API technology.

(ii) Rights to access and use API technology.

(A) An API Technology Supplier must have and, upon request, must grant to API Data Providers and their API Users all rights that may be reasonably necessary to access and use API technology in a production environment, including:

(1) For the purposes of developing products or services that are designed to be interoperable with the API Technology Supplier's health information technology or with health information technology under the API Technology Supplier's control;

(2) Any marketing, offering, and distribution of interoperable products and services to potential customers and users that would be needed for the API technology to be used in a production environment; and

(3) Enabling the use of the interoperable products or services in production environments, including accessing and enabling the exchange and use of electronic health information.

(B) An API Technology Supplier must not condition any of the rights described in paragraph (a)(4)(ii)(A) of this section on the requirement that the recipient of the rights do, or agree to do, any of the following:

(1) Pay a fee to license such rights, including but not limited to a license fee, royalty, or revenue-sharing arrangement.

§ 170.404 Application programming interfaces (Condition and Maintenance of Certification)
(2) Not compete with the API Technology Supplier in any product, service, or market. (3) Deal exclusively with the API Technology Supplier in any product, service, or market. (4) Obtain additional licenses, products, or services that are not related to or can be unbundled from the API technology. (5) License, grant, assign, or transfer any intellectual property to the API Technology Supplier. (6) Meet additional developer or product certification requirements. (7) Provide the API Technology Supplier or its technology with reciprocal access to application data. (iii) Service and support obligations. An API Technology Supplier must provide all support and other services reasonably necessary to enable the effective development, deployment, and use of API technology by API Data Providers and their API Users in production environments. (A) Changes and updates to API technology. An API Technology Supplier must make reasonable efforts to maintain the compatibility of its API technology and to otherwise avoid disrupting the use of API technology in production environments. (B) Changes to terms and conditions. Except as exigent circumstances require, prior to making changes or updates to its API technology or to the terms and conditions thereof, an API Technology Supplier must provide notice and a reasonable opportunity for its API Data Provider customers and registered application developers to update their applications to preserve compatibility with API technology and to comply with applicable terms and conditions. (b) Maintenance of Certification. (1) Registration for production use. An API Technology Supplier with health IT certified to the certification criterion adopted in § 170.315(g)(10) must register and enable all applications for production use within 1 business day of completing its verification of an application developer's authenticity, pursuant to paragraph (a)(2)(ii)(C) of this section. (2) Service Base URL publication. API Technology Supplier must support the publication of Service Base URLs for all of its customers, regardless of those that are centrally managed by the API Technology Supplier or locally deployed by an API Data Provider, and make such information publicly available (in a computable format) at no charge. (3) Rollout of (g)(10)-Certified APIs. An API Technology Supplier with API technology previously certified to the certification criterion in § 170.315(g)(8) must provide all API Data Providers with such API technology deployed with API technology certified to the certification criterion in § 170.315(g)(10) within 24 months of this final rule's effective date.
Preamble FR Citation: 84 FR 7485-95 **Specific questions in preamble?** *Yes*
Regulatory Impact Analysis: Please see 84 FR 7570-75 for estimates related to this proposal.
Public Comment Field: CTA supports the general proposition that connecting to an API should not be cost-prohibitive and should not be used as a means of information blocking. Patients should have free access to their electronic health information through APIs. We believe that HIPAA's limitation on fees that

can be charged to a patient at 45 C.F.R. § 164.524(c)(4) already appropriately safeguards patients from inappropriate fees and provides a mechanism to enforce such free access, and we have concern that adding additional fee restrictions on top of HIPAA's will cause confusion and unnecessary burden.

With respect to other actors in the API ecosystem – API Technology Suppliers, API Data Providers, and API Users – we recommend that ONC avoid placing restrictions on fees that may be charged between these parties in order to allow for a robust, free-market economy to continue to develop. ONC should only intervene with respect to charges when actions rise to the level of information blocking.

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: In general, CTA supports ONC's proposal and believes that it is necessary to improve information sharing practices that are currently impeding the ability for patients to obtain and share their health information, and believes that ONC has narrowly crafted reasonable exceptions to the general prohibition.

§ 171.102 Definitions

For purposes of this part:

Access means the ability or means necessary to make electronic health information available for use, including the ability to securely and efficiently locate and retrieve information from any and all source systems in which the information may be recorded or maintained.

Actor means a health care provider, health IT developer of certified health IT, health information exchange, or health information network.

API Data Provider is defined as it is in § 170.102.

API Technology Supplier is defined as it is in § 170.102.

Electronic Health Information (EHI) means—

(1) Electronic protected health information; and

(2) Any other information that 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 is transmitted by or maintained in electronic media, as defined in 45 CFR 160.103, that 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.

Electronic media is defined as it is in 45 CFR 160.103.

Electronic protected health information (ePHI) is defined as it is in 45 CFR 160.103.

§ 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:

While CTA understands the importance of prohibiting information blocking, CTA believes that the terms "health information network" and "health information exchange" are defined too broadly and, therefore, capture entities far outside the intent of the statute. For example, a cloud service provider that offers data-agnostic storage and processing services may be used to share electronic health information between unaffiliated parties and, as a result, may be deemed an entity that "[p]rovides … [a] service that enables or facilitates the access [or] exchange … of electronic health information between or among two or more unaffiliated individuals or entities." The cloud services provider may not even know that it is handling electronic health information. Likewise, a telecommunications provider that transmits data without regard to the content of the data may be considered to be facilitating the exchange of data, including electronic health information, between or among two or more unaffiliated individuals or entities. Including such entities within the definitions of "health information network" and "health information exchange" is contrary to the plain meaning of the terms (since such facilities are not focused on health information) and may lead to unintended consequences—such as currently-legal practices that are data agnostic becoming "information blocking." To address this issue, CTA recommends revising the definitions to individuals and entities that facilitate the access, exchange, or use of primarily electronic health information, but explicitly exempt entities that access, exchange, or use information without regard to whether the information is health-related. CTA also recommends that a consumer using an app to access their own health record from a health care organization, health information exchange or health niformation network and shares it with a third party (such as a caregiver) is exempt from the information blocking provisions.

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: CTA supports making price information publicly available through APIs. Consumers are used to leveraging technology in other sectors to compare prices. Similarly, patients should have the ability to leverage technology in the health care sector to readily compare prices for different providers and different procedures. This can only be done by broadly defining electronic health information to include price information, creating standardized access to such information through APIs, and prohibiting health plans and others from trying to block access to price information through unreasonable contractual restrictions or otherwise.

VIII.D Proposed Exceptions to the Information Blocking Provision

§ 171.201 Exception – Preventing harm

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

(a) The actor must have a reasonable belief that the practice will directly and substantially reduce the likelihood of harm to a patient or another person arising from—

(1) Corrupt or inaccurate data being recorded or incorporated in a patient's electronic health record;

(2) Misidentification of a patient or patient's electronic health information; or

(3) Disclosure of a patient's electronic health information in circumstances where a licensed health care professional has determined, in the exercise of professional judgment, that the disclosure is reasonably likely to endanger the life or physical safety of the patient or another person, provided that, if required by applicable federal or state law, the patient has been afforded any right of review of that determination.

(b) If the practice implements an organizational policy, the policy must be—

(1) In writing;

(2) Based on relevant clinical, technical, and other appropriate expertise;

(3) Implemented in a consistent and non-discriminatory manner; and

(4) No broader than necessary to mitigate the risk of harm.

(c) If the practice does not implement an organizational policy, an actor must make a finding in each case, based on the particularized facts and circumstances, and based on, as applicable, relevant clinical, technical, and other appropriate expertise, that the practice is necessary and no broader than necessary to mitigate the risk of harm.

Preamble FR Citation: 84 FR 7523-26 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

While CTA is generally supportive of this exception, we recommend that ONC specify a timeframe and mechanism for this harm to be addressed and resolved by stakeholders so that it cannot be claimed unilaterally and indefinitely by the entity asserting the exception. For example, if an entity claims that a disclosure would cause harm, the requesting entity should be able to appeal the decision to ONC or to some other neutral body within 90 days, and the entity claiming harm should be required to make the disclosure if the neutral party disagrees that the disclosure would cause harm.

§ 171.202 Exception – Promoting the privacy of electronic health information

To qualify for this exception, each practice by an actor must satisfy at least one of the sub-exceptions in paragraphs (b) through (e) of this section at all relevant times.

(a) Meaning of "individual" in this section. The term "individual" as used in this section means one or more of the following—

(1) An individual as defined by 45 CFR 160.103.

(2) Any other natural person who is the subject of the electronic health information being accessed, exchanged, or used.

(3) A person who legally acts on behalf of a person described in paragraph (a)(1) or (2) of this section, including as a personal representative, in accordance with 45 CFR 164.502(g).

(4) A person who is a legal representative of and can make health care decisions on behalf of any person described in paragraph (a)(1) or (2) of this section.

(5) An executor, administrator or other person having authority to act on behalf of a deceased person described in paragraph (a)(1) or (2) of this section or the individual's estate under State or other law.

(b) Precondition not satisfied. If the actor is required by a state or federal privacy law to satisfy a condition prior to providing access, exchange, or use of electronic health information, the actor may choose not to provide access, exchange, or use of such electronic health information if the precondition has not been satisfied, provided that—

(1) The actor's practice—

(i) Conforms to the actor's organizational policies and procedures that:

(A) Are in writing;

(B) Specify the criteria to be used by the actor and, as applicable, the steps that the actor will take, in order that the precondition can be satisfied; and

(C) Have been implemented, including by taking reasonable steps to ensure that its workforce members and its agents understand and consistently apply the policies and procedures; or

(ii) Has been documented by the actor, on a case-by-case basis, identifying the criteria used by the actor to determine when the precondition would be satisfied, any criteria that were not met, and the reason why the criteria were not met; and

(2) If the precondition relies on the provision of consent or authorization from an individual, the actor:

(i) Did all things reasonably necessary within its control to provide the individual with a meaningful opportunity to provide the consent or authorization; and

(ii) Did not improperly encourage or induce the individual to not provide the consent or authorization.

(3) The actor's practice is—

(i) Tailored to the specific privacy risk or interest being addressed; and

(ii) Implemented in a consistent and non-discriminatory manner.

c) Health IT developer of certified health IT not covered by HIPAA. If the actor is a health IT developer of certified health IT that is not required to comply with the HIPAA Privacy Rule when engaging in a practice that promotes the privacy interests of an individual, the actor may choose not to

§ 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:

CTA generally agrees with the proposal to permit information blocking for valid security purposes, but requests that ONC clarify that where there are a significant imbalance in resources between the data holder and the requesting entity, the entity with the larger capacity to implement robust security measures cannot set policies for addressing security issues that would be impractical for the smaller entity to meet.

§ 171.207 Exception – Maintaining and improving health IT performance

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

(a) Maintenance and improvements to health IT. An actor may make health IT under its control temporarily unavailable in order to perform maintenance or improvements to the health IT, provided that the actor's practice is—

(1) For a period of time no longer than necessary to achieve the maintenance or improvements for which the health IT was made unavailable;

(2) Implemented in a consistent and non-discriminatory manner; and

(3) If the unavailability is initiated by a health IT developer of certified health IT, HIE, or HIN, agreed to by the individual or entity to whom the health IT developer of certified health IT, HIE, or HIN supplied the health IT.

(b) Practices that prevent harm. If the unavailability of health IT for maintenance or improvements is initiated by an actor in response to a risk of harm to a patient or another person, the actor does not need to satisfy the requirements of this section, but must comply with all requirements of § 171.201 at all relevant times to qualify for an exception.

(c) Security-related practices. If the unavailability of health IT for maintenance or improvements is initiated by an actor in response to a security risk to electronic health information, the actor does not need to satisfy the requirements of this section, but must comply with all requirements of § 171.203 at all relevant times to qualify for an exception.

Preamble FR Citation: 84 FR 7550-52 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

CTA generally supports this exception, but requests that ONC require the data holder to communicate an estimated timeframe for the completion of the maintenance and should inform the requestor of any circumstances that later arise that will cause the data holder to exceed the quoted timeframe.

Section X – Patient Matching Request for Information

Opportunities to Improve Patient Matching
We seek comment on additional opportunities that may exist in the patient matching space and ways that ONC can lead and contribute to coordination efforts with respect to patient matching. ONC is particularly interested in ways that patient matching can facilitate improved patient safety, better care coordination, and advanced interoperability.
Preamble FR Citation: 84 FR 7554-55 **Specific questions in preamble?** *Yes*
Regulatory Impact Analysis: NA
Public Comment Field: CTA recommends looking at the new technologies that ONC identified, along with other potential new technologies, such as blockchain technology, to improve patient matching. CTA would be happy to assist ONC with identifying new technologies that may assist in the area of patient matching, as CTA's members are involved in cutting edge technologies that could potentially assist in this effort.