June 3, 2019

Donald W. Rucker, MD
National Coordinator for Health IT
Office of the National Coordinator
Department of Health and Human Services
Mary E. Switzer Building
330 C Street, SW, Office 7009A
Washington, D.C. 20201

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

Dear Dr. Rucker,

CommonWell Health Alliance (the "Alliance") appreciates the opportunity to submit comments regarding the 21st Century Cures Act, published on March 4, 2019. The Alliance appreciates the tremendous effort undertaken by the Office of the National Coordinator for Health IT in the preparation of this seminal set of draft rules, and we stand by ONC in its ongoing commitment to enable ubiquitous nationwide interoperability.

By way of background, CommonWell Health Alliance is a not-for-profit trade association made up of diverse health care and health IT stakeholders across the care continuum, dedicated to the notion that the individual's data should be available to themselves and their caregivers, regardless of where care has occurred. Alliance members represent more than 20 care settings, including technology leaders in acute care, ambulatory care, post-acute care, patient portals/PHRs, imaging, pharmacy, population health, emergency services and others; and other key organizations across the health care spectrum such as State and Federal Agencies, Not-For-Profit Organizations, and of course clinical providers. The Alliance and its members are committed to the belief that access to health data must be built into information technologies at a reasonable cost for use by a broad range of health care providers and by individuals to best manage their health. To that end, we have enabled secure, authorized, universal access to health data via a person-centered nationwide network. Over the past four years, we have driven adoption of nationwide interoperability among more than 13,000 care locations, enabling over 200 million transactions for more than 50 million unique enrolled patients.

[A] Structure of this Comment Letter

Although CommonWell Health Alliance is an association whose Members span the breadth of health IT, we are focused on a single vision and mission, namely to enable a vendor-neutral nationwide infrastructure that enables person-centered exchange. As such, although there is a broad swath of HIT and interoperability issues covered by the proposed rule – and a corresponding broad set of opinions held by the contributors to and reviewers of this comment letter – **we have focused our attention only on those issues that are germane to the vision and mission of the Alliance.** Our focus will largely be trained on the Information Blocking Exceptions (Section VIII); for further commentary on the other Sections from the perspective of Alliance Members, we recommend that ONC review our Members' individual comment letters.

Note that the comments in this letter are not intended to specifically endorse nor refute any commentary made by CommonWell Members or supporters through their own specific comment letters to ONC, except where specifically highlighted as such.

Finally, in Section D of this letter we extensively utilize the response template document published by ONC. We thank ONC for publishing this template as we found the tool to be exceedingly helpful for both structuring the final response as well as for coordinating the comment solicitation and review process across our stakeholders.

[B] Statement of Support

On the whole, CommonWell Health Alliance is very supportive of the goals and direction articulated by the Cures Act. We believe that the direction laid by The Cures Act itself and the set of rigorous exceptions detailed in the NPRM will have the overall effect of discouraging information blocking in the many forms that exists today. In informal terms, the "writing is on the wall for information blockers", and to the extent that this rule makes that abundantly clear to participants across the healthcare industry, we are very supportive of its enactment and enforcement.

[C] Overview of Feedback

Based on our experience, the most prevalent forms of information blocking stem from a limited set of root causes. We thematically outline those issues over here, and then refer back to them in the detailed commentary sections:

1. **Business and competitive reasons:** as we have sought to grow the Alliance, both HIT vendors and provider organizations alike have provided a variety of reasons for delay or refusal to participate. Many reasons are perfectly legitimate, and usually addressed over time; however on several occasions, we have encountered unambiguous information-blocking head-on: e.g., provider organizations who refuse to participate specifically because they are worried that "*their patient data"* will end up in the hands of competing providers in the same region, or HIT vendors who are concerned that increased interoperability will enable other HIT vendors to disintermediate them. In either case they cling to the patient data for competitive advantage and in so doing create barriers to sharing. It is our hope that these data-hoarding behaviors will be effectively disincentivized by virtue of this Information Blocking rule.

2. **HIPAA/Privacy misinformation:** where #1 above is an example of intentional information blocking, it is probably dwarfed by the volume of unintentional data blocking created by the pervasive lack of understanding of the "portability vs. privacy" intentions of HIPAA. Without a doubt, ONC and its sister agencies have made tremendous progress in clarifying the intent of HIPAA and creating complementary resources for patients, but our hope is that this rule will make it incumbent upon both HIT vendors and clinical provider organizations to thoughtfully and formally train their staff on the actual requirements, particularly where it comes to the rights for patients, for other clinical providers, and for other healthcare participants to request and receive patient health data.

3. **Security concerns:** we have witnessed and even had to confront a very different source of concern with information sharing: a lack of clarity on the degree of reliability – from the data stewardship and security perspectives – of the counterparty or participant (typically an HIT vendor) that wishes to exchange data. For example, when CommonWell opened up the Patient Access purpose of use, we encountered a broad variety of Personal Health Record (PHR) vendors and application developers. Determining the extent to which these parties were appropriately geared to access patient data has turned out to be more of an endeavor than we expected, largely because we found that the most-

commonly adopted security standards were simply not broad or deep enough to provide the level of assurance needed to enable exchange through a centralized interoperability service such as ours. Nor, alternatively, was there an industry-accepted authority to certify and validate the robustness of such technology participants. As such, we had to create a higher bar for participation in the network, balancing our security needs with the need for the bar to still be reasonable, achievable, and of course applicable in a non-discriminatory manner. Our hope is that national standards for data privacy and security practices will continue to expand beyond the prevailing practices so that other health information networks and data sources across the industry will not have to invest the efforts that we did in order to create robust security; and we of course will adjust our policies and requirements accordingly to meet the industry so that we can enable robust interoperability both within and outside our network.

4. **Lack of a reliable "escape hatch":** due to the tremendous size and heterogeneity of participants across the US healthcare landscape, the default universal "escape hatch" from information blocking is likely to be the lowest common denominator technology: i.e., printing paper charts. For the average provider organization – i.e., the resource-constrained community hospital or independent <100 practitioners' clinic – the sharing of paper charts is likely to be the predominant mechanism from escaping "information blocking ignominy". This is not just theory: this is in fact very much the empirical evidence witnessed by the entirety of the industry in response to the Meaningful Use Transitions of Care measure, which singlehandedly propelled astronomically high volumes of faxed patient charts – hardly the result that ONC was aiming for, but an easy-to-anticipate one nonetheless.

   To avoid a similar fate, it is critical that ONC succeed in its endeavor to drive adoption of a broadly-adopted electronic standards-based approach, easily built into HIT nationwide. The TEFCA Framework is an obvious choice. Viewed from this lens, TEFCA does not serve as an "exception" to information blocking per se – since it actually enables information flow rather than giving the record-holder an excuse not to share the data – but rather it acts as a reliable backstop for providers confronted with an infinite variety of potential permutations for patient clinical data requests. **In fact we would go so far as to suggest that participation in a QHIN should alleviate the burden of proof for the provider** when confronted with an information-blocking complaint, provided of course that the provider is in fact actively participating in the QHIN and that the option of accessing data through TEFCA (i.e., any QHIN) was actually provided back to the requester. We are not positing here that TEFCA should be the only escape hatch – for example, in some circumstances, a vertical standards-based API that directly accesses the data repository (as opposed to TEFCA, which creates a horizontal network across repositories) may be a more appropriate or equally acceptable solution – but that it is clear that the information blocking approach should provide such mechanisms so that a clinical data holder can be assured that they actually ***can*** reasonably fulfill any appropriate information request as required by The Cures Act.

We refer back to these cross-cutting themes in the course of our structured responses below.

[D] Feedback

Section VII – Conditions and Maintenance of Certification

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: As an aspiring Qualified Health Information Network (QHIN), we believe that all healthcare participants should participate in TEFCA. However, we do not recommend that TEFCA be a hard requirement for HIT vendors, because such a heavy-handed approach will inevitably lead to a check-the-box approach from vendors and possibly to chaos, with the long-tail of HIT vendors doubtlessly paying the price of rushing into TEFCA by connecting to a host of QHINs artificially propped-up by profiteers anticipating a windfall. In other words, a hard requirement to participate in TEFCA may precipitate the unnecessary churn and burn that the well-meaning ONC State HIE Initiative engendered during the 2010-2017 timeframe, which is a waste of industry resources and would probably undermine the long-term success (real and perceived) of TEFCA. On the other hand, as per the earlier discussion on TEFCA as an "escape hatch", we **do** advocate for ONC to explicitly state that a TEFCA-based response to an information request would be recognized as an acceptable alternative provided by a responder to a requestor who seeks non-standard means of access to data. In other words, if a request for access comes in one form and could be met by use of TEFCA, insistence by the requestor that access should be enabled by an alternate approach should not be considered an act of information blocking by the HIT developer.

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:

We support this Exception as is. While we have no specific recommendations at this time, we do have some reservations as to how it will be implemented. Historically, there has been a concern that some clinical institutions use "preventing patient harm" as an excuse to cherry-pick trading partners with whom clinical data would be exchanged. However, this Exception as written emphasizes the adherence to a consistent written policy applied in a non-discriminatory fashion, or else an explicit justification for not sharing the data – in our view, such requirements **should be** a sufficient deterrent of disingenuous information-blocking practices, and instead motivate the behavior that is more conducive to the end goal espoused by ONC (and by the Alliance), but implementation of this will be worth **monitoring** post hoc.

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

§ 171.202 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:

We support this Exception, but seek additional clarity to be added to the requirement. In particular, this rule emphasizes that data sharing may be constrained per an organization's policies, as long as those policies are applied in a non-discriminatory manner. Our concern is that an organization's policy may actually be uniformly blocking the exchange of information and yet still meet the word of this requirement, simply because it did so in a non-discriminatory manner. From our perspective, it is important that an instance of information blocking that traces back to an organization's self-determined policy should in turn open the door for the policy itself to be examined through the lens of information blocking.

§ 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:

We support this Exception. In fact, we support this Exception not only in terms of this NPRM, but as a practical matter we have had to create policies that align with this Exception. Going back to our initial preamble about "Security" as one of the roots of information blocking, we expound here that there are two current failings in the "app" business that is gaining a foothold in healthcare: a failure of any reliable governance body to be able to vet and/or certify apps for trustworthiness; and a failure of any governance body to ensure that users of these apps (especially individual patients and their guardians) are appropriately explained the purpose and consequences of sharing data with the app. To solve the first of these issues, the Alliance has instituted an increasing "bar" of security and certification requirements that are explicitly codified in our Specifications; however we have not yet tackled the latter concern, historically deferring instead to other complementary patient-centered organizations such as the National Association for Trusted Exchange (NATE). Given a lack of sufficiently-rigorous generally-applicable security requirements and appropriate user/consumer education – which are diametrically at odds with the monumental risks created by a security breach and a breach in confidence, respectively – we anticipate that this Exception may become a recurring source of claimed Exceptions to data blocking, even by institutions in otherwise good standing. We

strongly advise ONC to focus an investment of federal effort from the complementary perspectives of security technology (likely through NIST and ONC itself) as well as privacy policy and consumer protection (likely through OIG and OCR) on these issues.

171.204 Exception – Recovering costs reasonably incurred

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

(a) Types of costs to which this exception applies. This exception is limited to the actor's costs reasonably incurred to provide access, exchange, or use of electronic health information.

(b) Method for recovering costs. The method by which the actor recovers its costs—

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

(2) Must be reasonably related to the actor's costs of providing the type of access, exchange, or use to, or at the request of, the person or entity to whom the fee is charged;

(3) Must be reasonably allocated among all customers to whom the technology or service is supplied, or for whom the technology is supported;

(4) Must not be based in any part on whether the requestor or other person is a competitor, potential competitor, or will be using the electronic health information in a way that facilitates competition with the actor; and

(5) Must not be based on the sales, profit, revenue, or other value that the requestor or other persons derive or may derive from the access to, exchange of, or use of electronic health information, including the secondary use of such information, that exceeds the actor's reasonable costs for providing access, exchange, or use of electronic health information.

(c) Costs specifically excluded. This exception does not apply to—

(1) Costs that the actor incurred due to the health IT being designed or implemented in non-standard ways that unnecessarily increase the complexity, difficulty or burden of accessing, exchanging, or using electronic health information;

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

(3) Opportunity costs, except for the reasonable forward-looking cost of capital;

(4) A fee prohibited by 45 CFR 164.524(c)(4);

(5) A fee based in any part on the electronic access by an individual or their personal representative, agent, or designee to the individual's electronic health information;

(6) A fee to perform an export of electronic health information via the capability of health IT certified to § 170.315(b)(10) of this subchapter for the purposes of switching health IT or to provide patients their electronic health information; or

(7) A fee to export or convert data from an EHR technology, unless such fee was agreed to in writing at the time the technology was acquired.

(d) Compliance with the Conditions of Certification.

§ 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:

Our belief is that interoperability needs to be commoditized, which implies a marginal cost model that converges to zero at the limit, and as such we support this Exception. However it is hard to determine the legitimacy of all forms of business models a priori, and we suggest that ONC include further examples of good and bad models – for a variety of different interoperability participants, from QHINs to EHRs to clinical providers – to clarify this Exception.

171.205 Exception – Responding to requests that are infeasible

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

(a) Request is infeasible.

(1) The actor must demonstrate, in accordance with paragraph (a)(2) of this section, that complying with the request in the manner requested would impose a substantial burden on the actor that is unreasonable under the circumstances, taking into consideration—

(i) The type of electronic health information and the purposes for which it may be needed;

(ii) The cost to the actor of complying with the request in the manner requested;

(iii) The financial, technical, and other resources available to the actor;

(iv) Whether the actor provides comparable access, exchange, or use to itself or to its customers, suppliers, partners, and other persons with whom it has a business relationship;

(v) Whether the actor owns or has control over a predominant technology, platform, health information exchange, or health information network through which electronic health information is accessed or exchanged;

(vi) Whether the actor maintains electronic protected health information on behalf of a covered entity, as defined in 45 CFR 160.103, or maintains electronic health information on behalf of the requestor or another person whose access, exchange, or use of electronic health information will be enabled or facilitated by the actor's compliance with the request;

(vii) Whether the requestor and other relevant persons can reasonably access, exchange, or use the electronic health information from other sources or through other means; and

§ 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:

We support this Exception. In particular, while our operational focus has been trained on the potential for the sources of data to act as information blockers, the reverse is certainly true, i.e., that requesters of data can also deliberately or inadvertently create barriers to exchange through the infeasibility and intransigence of their requests. There has to be a middle ground, and this Exception provides a solid basis for it.

However, we suggest two modifications that ONC should consider, either directly within this Exception or in the larger context of this NPRM. First of all, per our previous "escape hatch" discussion, it should be incumbent on the data source (e.g., EHR) or exchange facilitator (e.g., HIN) to provide reasonable alternatives to fulfill the request for the data, and it is in turn incumbent on ONC to provide guidance on acceptable alternatives, so that both parties (requestors and responders) are on equal footing regardless of relative economic strength. Again, a TEFCA-compliant mechanism is our leading example for such an alternative, but there probably should be a shortlist of other equally-acceptable standards-based mechanisms.

Secondly, we believe that this Exception grants too much leeway to smaller entities to get away with information blocking. While historical programs for nationwide data exchange have generally been embraced only by the larger hospitals and health systems due to the financial burdens those programs imposed, that is no longer the reality. In addition to CommonWell and

to Carequality, both of whom enable highly affordable (often free) information-sharing capabilities built into EHRs for tens of thousands of clinics nationwide, there are also numerous for-profit data sharing networks, platforms and intermediaries today that enable provider organizations across the spectrum (even those without an EHR!) to be able to share clinical data. So while we agree that some degree of inequality in application of this Exception is inevitable, we **strongly** caution ONC from ostensibly giving smaller provider practices and smaller EHR vendors a "free pass" when the world of data exchange has dramatically shifted in their favor.

§ 171.206 Exception – Licensing of interoperability elements on reasonable and non-discriminatory terms

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

(a) Responding to requests. Upon receiving a request to license or use interoperability elements, the actor must respond to the requestor within 10 business days from receipt of the request by:

(1) Negotiating with the requestor in a reasonable and non-discriminatory fashion to identify the interoperability elements that are needed; and

(2) Offering an appropriate license with reasonable and non-discriminatory terms.

(b) Reasonable and non-discriminatory terms. The actor must license the interoperability elements described in paragraph (a) of this section on terms that are reasonable and non-discriminatory.

171.206 Exception – Licensing of interoperability elements on reasonable and non-discriminatory terms

(1) Scope of rights. The license must provide all rights necessary to access and use the interoperability elements for the following purposes, as applicable.

(i) Developing products or services that are interoperable with the actor's health IT, health IT under the actor's control, or any third party who currently uses the actor's interoperability elements to interoperate with the actor's health IT or health IT under the actor's control.

(ii) Marketing, offering, and distributing the interoperable products and/or services to potential customers and users.

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

(2) Reasonable royalty. If the actor charges a royalty for the use of the interoperability elements described in paragraph (a) of this section, the royalty must be reasonable and comply with the following requirements.

(i) The royalty must be non-discriminatory, consistent with paragraph (b)(3) of this section.

(ii) The royalty must be based solely on the independent value of the actor's technology to the licensee's products, not on any strategic value stemming from the actor's control over essential means of accessing, exchanging, or using electronic health information.

(iii) If the actor has licensed the interoperability element through a standards development organization in accordance with such organization's policies regarding the licensing of standards-essential technologies on reasonable and non-discriminatory terms, the actor may charge a royalty that is consistent with such policies.

(3) Non-discriminatory terms. The terms (including royalty terms) on which the actor licenses and otherwise provides the interoperability elements must be non-discriminatory and comply with the following requirements.

(i) The terms must be based on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests.

(ii) The terms must not be based in any part on—

(A) Whether the requestor or other person is a competitor, potential competitor, or will be using electronic health information obtained via the interoperability elements in a way that facilitates competition with the actor; or

(B) The revenue or other value the requestor may derive from access, exchange, or use of electronic health information obtained via the interoperability elements, including the secondary use of such electronic health information.

(4) Collateral terms. The actor must not require the licensee or its agents or contractors to do, or to agree to do, any of the following.

(i) Not compete with the actor in any product, service, or market.

(ii) Deal exclusively with the actor in any product, service, or market.

(iii) Obtain additional licenses, products, or services that are not related to or can be unbundled from the requested interoperability elements.

§ 171.206 Exception – Licensing of interoperability elements on reasonable and non-discriminatory terms

(iv) License, grant, assign, or transfer to the actor any intellectual property of the licensee.

(v) Pay a fee of any kind whatsoever, except as described in paragraph (b)(2) of this section, unless the practice meets the requirements of the exception in § 171.204.

(5) Non-disclosure agreement. The actor may require a reasonable non-disclosure agreement that is no broader than necessary to prevent unauthorized disclosure of the actor's trade secrets, provided—

(i) The agreement states with particularity all information the actor claims as trade secrets; and

(ii) Such information meets the definition of a trade secret under applicable law.

(c) Additional requirements relating to the provision of interoperability elements. The actor must not engage in any practice that has any of the following purposes or effects.

(1) Impeding the efficient use of the interoperability elements to access, exchange, or use electronic health information for any permissible purpose.

(2) Impeding the efficient development, distribution, deployment, or use of an interoperable product or service for which there is actual or potential demand.

(3) Degrading the performance or interoperability of the licensee's products or services, unless necessary to improve the actor's technology and after affording the licensee a reasonable opportunity to update its technology to maintain interoperability.

(d) Compliance with conditions of certification. Notwithstanding any other provision of this exception, if the actor is a health IT developer subject to the conditions of certification in §§ 170.402, 170.403, or 170.404 of this subchapter, the actor must comply with all requirements of such conditions for all practices and at all relevant times.

Preamble FR Citation: 84 FR 7544-50 **Specific questions in preamble?** *Yes*

Regulatory Impact Analysis: Not applicable

Public Comment Field:

While we support this Exception and believe that a RAND-based licensing agreement is appropriate for driving ubiquity of interoperability, we have feedback about the timing. In particular, the postulated "10 days" timeframe likely will not be enough as an actor may not realize that a request may require a licensing arrangement; or the actor may discover that such IP was not designed in the first place to be "license-ready", e.g., the software may be wedded to other proprietary technologies that may not have any bearing on these interoperability elements, and thus additional work is needed to separate them and determine a path to providing a RAND option.

§ 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:

We strongly support this Exception. One clarification we suggest that is made to this Exception is the notion of security events or other such events that require unexpected downtime. On the one hand, events such as these should obviously not be subject to information blocking, as the stakes for broad erosion of trust or even patient safety can be at risk; on the other hand, it is reasonable for ONC to require that a protocol or process be explicitly articulated to inform users in the circumstance that such unanticipated events occur.

Request for information on a potential additional information blocking exception for complying with the Common Agreement for Trusted Exchange

We are considering whether we would should propose, in a future rulemaking, a narrow exception to the information blocking provision for practices that are necessary to comply with the requirements of the Common Agreement. Such an exception may support adoption of the Common Agreement and encourage other entities to participate in trusted exchange through HINs that enter into the Common Agreement. We ask commenters to provide feedback on this potential exception to the information blocking provision to be considered for inclusion in future rulemaking.

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

Regulatory Impact Analysis: Not applicable

Request for information on a potential additional information blocking exception for complying with the Common Agreement for Trusted Exchange

As per the earlier discussion, we believe that the ideal role for TEFCA in the context of information blocking is to provide an avenue through which healthcare participants can successfully meet the requirements of The Cures Act. As such, rather than treating it as an "Exception" per se – which implies that data is not being shared, whereas TEFCA enables quite the opposite – we advocate for applying TEFCA as a suitable ONC-approved "alternative mechanism" for complying with an information sharing request that is either ambiguous, ill-formed or else infeasible, i.e., as an alternative for those who would otherwise claim the Exception under "§ 171.205 – Responding to requests that are infeasible".

However, we also note that, to the extent that either the existing TEFCA NPRM Draft #2 (including the MRTCs - Minimum Required Terms and Conditions) or the future Common Agreement (as created by ONC and the RCE) includes requirements that are not met by the requester of data – such as requirements for user authentication, for example - that claiming an Exception under TEFCA may in fact be appropriate. One could argue that many of these Exceptions could fall under one of the existing Exceptions articulated in this NPRM; unfortunately the answer may be largely unknowable until the future development of the Common Agreement. We advise ONC to keep an open-minded approach as we begin that journey collectively as an industry.

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:

Patient Matching is a central concern to the success of CommonWell, and in general we support the research and recommendations of the Pew Charitable Trusts ("Pew") on this topic. Rather than re-stating their conclusions, we defer and endorse both their comments on this topic in response to this NPRM and to their published reports on this topic.

Separate from but still in line with the recommendations of Pew, we have five recommendations for ONC:

1. Drive standardization of commonly exchanged data elements through the various programs, policies and rulemaking mechanisms: in particular the patient's last name (e.g., by removing suffixes and special characters) and the patient's address (including zip code).
2. Drive adoption of two new demographic elements through the various programs, policies and rulemaking mechanisms: patient e-mail and patient cell phone number. These two demographic elements are largely ubiquitous, relatively constant across spans of time, and unique, thus making them ideal elements on which to match patients, if only they were more universally captured and exchanged for patient matching purposes. They also have the additional attribute of being verifiable in real-time, thus mitigating the chances of incorrect or inaccurate data capture.

   These first two recommendations are straightforward improvements that could improve nationwide patient matching **immediately**.

   In addition:

3. ONC should work with CMS, The Joint Commission, or otherwise to push providers to adopt process enhancements that would improve on patient matching within their own organization and across. For example, building on Recommendation #2 above, a validated cell phone number is increasingly worth the effort in terms of downstream savings, as care coordination and data sharing becomes more the norm than the exception – and these bodies can help to drive a more standardized registration process through which such quality data is obtained and validated in the first place.
4. ONC should study the opportunity to drive adoption of a more robust centrally managed identifiers, including strong identifiers such as drivers' licenses, which again are largely ubiquitous and unique, slightly less constant than cell phone numbers, but more authoritative as identifiers.
5. Finally, looking to the longer term, ONC should study the opportunity to utilize other patient-matching technologies such as biometrics, referential matching, and others recommended by Pew.

[E] Concluding Remarks

In conclusion, we remind ONC that CommonWell Health Alliance is dedicated to universal person-centered access to health data. As ONC embarks upon the journey to implement the Information Blocking provisions of The Cures Act, we hope that our feedback is perceived in light of our steadfast Mission to drive interoperability nationwide.

On behalf of the CommonWell Health Alliance, thank you again for the opportunity to comment on the *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program.* For more information, please contact me at jitin@commonwellalliance.org.

Respectfully submitted,

Jitin Asnaani
Executive Director
CommonWell Health Alliance