HIMSS Electronic Health Record Association

33 W Monroe, Suite 1700
Chicago, IL 60603
swillis@himss.org
Phone: 312-915-9518
Twitter: @EHRAssociation

February 20, 2018

Donald Rucker, MD
National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
200 Independence Avenue, SW
Washington, DC 20201

Dear Dr. Rucker,

On behalf of the more than 30 member companies of the Electronic Health Record Association (EHRA), we are pleased to offer our comments to the Office of the National Coordinator for Health Information Technology (ONC) on the 21st Century Cures Act (Cures) Trusted Exchange Framework and Common Agreement (TEFCA). We appreciate this opportunity to provide input on the establishment of a framework for the exchange of health data across networks.

EHRA members serve the vast majority of hospitals and ambulatory care organizations that use electronic health records (EHRs) and other health information technology to deliver high quality, efficient care to their patients. Our core objectives focus on collaborative efforts to accelerate health IT adoption, advance interoperability, and improve the quality and efficiency of care through the use of these important technologies.

Given the concerns outlined in our comments below and the broad scope of the TEFCA proposal, we recommend ONC review stakeholder comments and publish an additional TEFCA proposed draft that provides clarity on key issues and allows for additional stakeholder feedback.

As currently proposed by ONC, the TEFCA draft calls for aggressive timeframes for development and implementation of new standards without providing important details regarding testing mechanisms or clarity on how these new programs will be rolled out and coordinated with stakeholders. It is also unclear how the additional costs associated with participating in a Qualified Health Information Network (QHIN) will be allocated and what measures can be taken to ensure financial considerations do not disincentivize participation.

We believe additional clarity from ONC on these key components, followed by an additional opportunity for stakeholders to comment prior to finalization of policy, will advance the shared goal of expanded interoperability and support widespread participation in the TEFCA.

We support the goal to provide nationwide interoperability using networks as important building blocks. However, as it stands, the proposed Trusted Exchange Framework suggests creation of new networks to become a QHIN rather than growing existing networks into QHINs. We urge ONC to take the latter approach.

Much progress has been made to date through various initiatives such as eHealth Exchange, CommonWell Health Alliance (CommonWell), Carequality, and Strategic Health Information Exchange Collaborative (SHIEC) with strong participation by EHRA members. We believe that the current capabilities provide a solid starting point for the Trusted Exchange Framework, subsequently focusing on building cross-network capabilities, while harmonizing agreements across networks essential to consistent data access and exchange across those networks. This is of particular importance in the areas of identity proofing, authentication of connected systems, security, privacy, and the standards used to access and exchange data across the networks. The efforts in progress between Carequality and CommonWell to connect the respective participants is a prime example of successfully connecting diverse approaches.

Establishing a U.S. Core Data for Interoperability (USCDI) is essential and we appreciate taking a glidepath approach where data can be proposed to move into the required core data set once all relevant standards and implementation guides have been established. We defer to our members' individual responses for consideration of the timing when certain data classes are ready to be moved through the various stages. We suggest the USCDI, as it evolves over time, be an important aspect of defining situations where information blocking is not present, e.g., absence of the ability to access or exchange data outside the then-current USCDI, or the inability to access or exchange the data within the then-current USCDI using agreed to minimum set of standards and implementation guides.

Overall, we are concerned that the proposed approach does not continue to build on the current state, but rather suggests a drastic change from diverse, yet increasingly connected architectures to a singular, monolithic architecture in a very short time period. We strongly believe that a step-wise approach would allow for the necessary pilot testing called out in the 21st Century Cures Act to validate whether the proposed architectural elements will work. For example, while we have substantial experience in both brokered and non-brokered document exchange using broadcast and directed queries, no such experience exists for brokered data element level access using APIs. A subset of the suggested capabilities may be sufficient and effective to achieve the intended access to the USCDI.

We agree that the Recognized Coordinating Entity (RCE) has an important role to play and suggest that the RCE collaborates with (emerging) QHINs and other stakeholders to establish a roadmap that starts with current state, identifies the critical use cases to focus on next, and then establishes the necessary guidance for the technologies and standards to support those use cases. Such an approach allows for deploying architecture fit for purpose and adequate testing before widely deploying the agreed to

capabilities. The RCE must have a neutral, convening, facilitating role, thus should not have any direct or indirect ownership or financial interest in a QHIN, its participants, or other stakeholders.

EHRA looks forward to working with ONC, the RCE, (emerging) QHINs, and other stakeholders to make meaningful, substantive progress toward nationwide interoperability and offers the following considerations to be addressed in the next iteration of the proposed Trusted Exchange Framework and USCDI.

Modular and Optional Capabilities

Concern/Question:

The proposed Trusted Exchange Framework suggests all capabilities (combination of brokered, broadcast and directed queries, for documents and data elements, for one or more patients, for all permitted purposes, for all data classes in the USCDI) be supported by all QHINs, immediately (within 12 months). This creates a substantial on-ramp for aspiring QHINs considering the variance between current capabilities and required capabilities. Furthermore, when considering the potential use cases that each combination may support, it is unclear that every combination is relevant or best supported using the same technologies and standards. For example, brokered broadcast HL7 FHIR® APIs for data element level access does not seem a relevant combination to support any of the use cases contemplated, while supporting all capabilities for various permitted purposes seems not to have the same priority.

Examples of other capabilities we understand are mandatory for the QHIN to support are vocabulary mapping, consent management, and/or store source data. Requiring a QHIN to perform vocabulary mappings rather than the source or target of the query is not necessarily the most appropriate, nor is the QHIN engaging directly with the patient/consumer to support consent management.

Recommendations:

We suggest a more modular approach be pursued, one that supports a stepwise progression from today's capabilities, prioritizing use cases, and identifying applicable technologies and standards to support those use cases best. Also, we suggest that capabilities such as vocabulary mapping be optional for a QHIN, although they should not be prohibited from offering such capabilities. We suggest that establishing the appropriate modules and optionality of those modules is to be done by RCE in collaboration with the (emerging) QHINs and their participants as they progress.

Separation of Technology and Standards Specifications from a Common Agreement

Concern/Question:

The level of technology and standards capabilities are too specific to be managed through the proposed Common Agreement. For example, the proposed capabilities and standards suggest that multi-patient document and data element level queries use the IHE Document Exchange Profiles for documents and FHIR for data element level APIs. We are concerned that the existing profiles do

not support multi-patient document queries and believe such queries initially could be satisfied using multiple single-patient queries. For data elements, the necessary implementation guides for population level queries do not yet exist while initial connectathons have just started. As these standards and implementation guides become available and agreed upon, the Common Agreement should not have to be updated every time. Current approaches indicate that this is more successfully managed by reference.

Recommendations:
We suggest that the technology and standards specifications be addressed outside of any Common Agreement, but rather through a set of RCE governed documents that are referenced from the Common Agreement as an umbrella to specific standards and technologies for supported use cases. This will help stabilize the Common Agreement, while the implementation guidance can adjust as technologies and standards evolve and use cases are expanded over time.

Source of Truth for Technologies and Standards

Concern/Question:
The proposed Trusted Exchange Framework references multiple potential sources for standards and technologies to be used by QHINs: Part B of the proposed Trusted Exchange Framework, the actual Common Agreement, 2015 Certification Edition for EHR Technology (CEHRT), and the Interoperability Standards Advisory (ISA).

The language, particularly under Principle 1.A. and Part B, Section 3, seems to imply that a QHIN (directly or through its participants) should implement all applicable standards in the ISA. We are very concerned with these ambiguous and indirect references as they dilute scope and introduce standards and implementation guides that, while perhaps applicable, are not suitable for immediate implementation, particularly considering that sources such as the ISA are not up-to-date and not necessarily inclusive of all applicable standards and implementation guides, nor are they fully applicable to QHIN-to-QHIN or network-to-network use cases.

Recommendations:
We suggest that not only references to specific technologies and standards are separated from a Common Agreement, but that such references are only made as an RCE implementation compendium directly, not through other potential sources.

We suggest that a QHIN should not have to adopt all standards and implementation guides referenced in the then-current Certification Edition or ISA. While they may serve as considerations for the RCE governance process to arrive at specific technologies and standards for particular use cases in scope, unless there is explicit agreement to its inclusion in the RCE implementation compendium, it should not be required for such use cases by the QHIN. Additionally, this will recognize that not all QHIN participants use certified solutions (particularly any care setting beyond inpatient and ambulatory, as well as any non-care organization such as registries, payers,

researchers, consumers, etc.). Such an approach will have the opportunity to be more responsive to the then-current state of technology and standards adoption.

Consequently, we suggest that the RCE establishes the necessary and relevant robust testing tools to validate adherence to the agreed-to standards and implementation guides rather than using the mechanism of a regulatory certification edition. We suggest, therefore, that certification to 2015 Certification Edition is not a prerequisite for participation in a QHIN, as the testing tools with supporting attestation can manage the necessary conformance. This would avoid creating inequity among participants where some would have to be certified and others would not in the absence of certification programs that address all types of participants.

Security Mechanisms for Network-to-Network Connections

Concern/Question:
The focus of the security/authentication capabilities is primarily focused on that involving authentication of individuals. While important for the QHIN participants, QHINs mostly will focus on system-to-system trust.

Recommendations:
We suggest that the RCE collaborate with (emerging) QHINs to establish appropriate system-to-system authentication capabilities. ONC should consider that QHIN participants primarily focus on identity proofing and requiring QHINs to take that on as well is unnecessary.

Reciprocity of Data Access and Exchange

Concern/Question:
The proposed Trusted Exchange Framework Part B, Section 5.3, suggests that there are no requirements of a QHIN to pay any amounts to another QHIN. Particularly in examples where a QHIN is able to request data, but not respond to data requests, inequities can occur where not all participants share reasonably in the cost of the national infrastructure.

For example, consider a scenario where two participants are on the network. Participant 1 has made substantial investments in the wise use of network traffic; selecting software which uses caching and incremental loading of data and other technical tools to wisely retrieve data when it is needed and is parsimonious in the use of network traffic. Alternatively, Participant 2 uses an app which was programmed incautiously and has a flaw where it requests data refreshes every millisecond at a rate far in excess of how it could ever use the data.

Participant 2 is generating network traffic far in excess of Participant 1 and placing a significant burden on Participant 2's own QHIN, Participant 1's QHIN, and on Participant 1's systems. To keep the network available and to incentivize appropriate use of the network, QHIN 1 and QHIN 2 should be able to charge Participant 2 proportionate to its usage of the network, so that Participant 2 is

incentivized to select apps and tools that are implemented well and do not create excessive traffic. Otherwise, Participant 1 is effectively subsidizing Participant 2's poor programming.

Additionally, while we understand that data access for individuals should be at no charge and support this requirement for individuals accessing their own data for their own use, we are concerned about data access on behalf of individuals that is not just for individual access but for other purposes, even when the individual has provided permission for it.

Our concern is that such participation does not reasonably share in the cost where the secondary use yields opportunities to monetize on that data access. For example, Individual A accesses their most current data through his/her App provider to review his/her latest image and lab results. This is a clear use case for individual access for which there should not be a charge. However, a more challenging situation is where Individual B has given permission to Company X to use his/her data for research, which in turn is commercialized through decision support offerings, new consumer Apps for consumers, and so on. Company X queries for all individuals for whom they have such permission and would not have to pay for queries going beyond the QHIN they participate in (and said QHIN could be made up only of organizations just like Company X). We are concerned that Company X and similar organizations would not reasonably share the cost for the infrastructure to enable such queries for uses beyond the individual.

While we recognize the appropriateness of free access for certain permitted purposes for certain stakeholders, the question then is what incentivizes these stakeholders to participate in the network without unduly burdening the system through unintended overuse.

Recommendations:
We suggest, particularly in the early phases as business models evolve, that the Trusted Exchange Framework be based on reciprocity of the ability to share data and, particularly in the absence of such ability, to allow payment for access and exchange. Not permitting QHINs to reasonably charge other QHINs proportionate to the infrastructure use of the QHIN and its participants' traffic may result in patients being unreasonably charged for access to their own records. That is not the intent, and we think that this could be reasonably addressed by a policy which permits QHINs to charge each other while allowing a certain number of free accesses/uses for patients for their own personal use, e.g., 365 a year.

Data Throttling and Spamming

Concern/Question:
We agree with the principle of non-discriminatory, consistent data access. However, not all data access can be equal, e.g., bulk data requests for payment versus patient record requests for treatment.

Recommendations:
We suggest that accommodations be made to prioritize network traffic across permitted purposes and other categories, with no discriminatory policies within such categories, while allowing for identification of abnormal, non-legitimate requests to avoid system degradation for valid use. Neither practice should be considered information blocking.

USCDI Specifications

Concern/Question:
The proposed USCDI data classes are not at a level of specification sufficient to implement. References to HL7 FHIR and C-CDA® are an improvement to some extent, but more specific references to implementation guide versions are required. Although the focus is on access and exchange using C-CDA and FHIR, for the document space there is no recognition of data available in other formats.

Additionally, different use cases may determine USCDI data class readiness. For example, in the case of single patient access or multi-patient bulk access, standards and implementation guidance have progressed further for single patient access to be part of the core data set, while requiring more work for multi-patient bulk access. For that use case, bulk exchange using FHIR resources has not been fully defined, nor does IHE Document Exchange support document requests for multiple patients. Additionally, data sources may require infrastructure upgrades to support such queries.

Recommendations:
We suggest that the RCE work closely with HL7, in particular, to evolve both C-CDA and FHIR U.S. Core implementation guidance evenly and ensure a data class can be represented with the same level of granularity and specificity in either a C-CDA document or a FHIR profile.

Also, we suggest that exchange of non-C-CDA documents, while progressively being discouraged, should not be a barrier to adoption in the initial stages. Rather, we suggest starting with the exchange of PDF documents, since we have that ability already; meanwhile, the participant moves toward C-CDA implementations versus not being able to connect at all.

We suggest that incentives be put in place to move toward more structured/granular data expressed through C-CDA and FHIR, e.g., presence of a migration plan, separate incentive programs, etc.

Lastly, we suggest that the USCDI progression from emerging to candidate to core be stratified by use cases to accommodate variations in technologies and standards necessary to support those use cases.

Patient Matching

Concern/Question:

While we appreciate a focus on patient matching and the need to exchange sufficient demographic data to support patient matching, we are concerned this is specified too much in the proposed Common Agreement language and less in the responsibilities of the RCE implementation compendium.

Recommendations:

We suggest that the specificity of what demographic data to exchange in support of patient matching be provided in an RCE implementation compendium rather than in the Common Agreement, similar to other standards. Also, we suggest that the RCE work with QHINs, as well as HHS, on best practices and guidance on how to enhance patient matching and particularly address the challenges of false positives that will remain a reality until such time a common, shared, unique patient identifier is established with robust patient matching processes at the front-end, where patients interact with the end-users.

Principles

Concern/Question:

We generally agree with the intent of the principles at the header levels, but suggest that the principles should remain principles, not implementation specifications. We observe that Principle 4 overlaps with Principle 2C, while the privacy and security considerations do not stand out as much as they should. Additionally, Principle 6 appears to address techniques to achieve the principle rather than the intent (e.g., population level bulk transfer).

Recommendations:

We suggest combining the consent related principle statements into Principle 4, which enables Principle 2 to focus on the fundamental business practices around transparency. Furthermore, we suggest that consent management is sensitive to the permitted purpose. Such clarification will help subsequent identification of standards to ensure such variations can be communicated across the networks. We suggest creating a new principle that focuses on privacy and security more specifically. Lastly, we suggest removing implementation guidance/assumptions from the principles and let the RCE drive the appropriate implementation approach in collaboration with the QHINs.

Timelines

Concern/Question:

The proposed timelines (12 months or less) appear overly aggressive for the scope envisioned. The USCDI, in contrast, lays out a more realistic approach, progressively extending the scope as standards and implementation guides for the data classes become available and are ready for wide deployment.

Recommendations:
We suggest that the Common Agreement defer the implementation timelines for the various capabilities to the RCE as part of a general governance process where use cases are prioritized; technologies and standards identified; pilot testing has been completed; and deployment is initiated based on use case specific considerations. Some use cases may progress more quickly than others that may require more time as standards and implementation guides may not yet be adequate for the number of participants that require new software and updated processes and/or for networks that need to adopt new capabilities.

Responsibilities and Definitions

Concern/Question:
Definitions of various roles/actors, e.g., QHIN, QHIN Participant, and End-User are ambiguous as they can be an organization, system, or individual. To understand responsibilities for capabilities, these definitions must be crisp and associated with the use cases and capabilities.

Recommendations:
We suggest clarification of the definitions and using distinct roles/actors for organizations, systems, and individuals. This approach will clearly assign responsibilities in the Common Agreement and particularly the RCE's implementation compendium to assign capabilities.

Data Storage by the QHIN

Concern/Question:
The language in Part B, Section 3, is ambiguous as to whether the QHIN is required to store detailed data (in document and/or data element form) for the USCDI beyond the MPI, RLS, and minimum metadata required to facilitate the core capabilities and audit log of the activities.

Recommendations:
We suggest clearly articulating that the QHIN has no obligation to store any data beyond MPI, RLS, and minimum metadata required to facilitate the core capabilities and audit log of the activities; however, observing that the QHIN is not prohibited from doing so should a QHIN wish to on behalf of its participants.

Rightsizing Data Request

Concern/Question:
While the proposed Trusted Exchange Framework does not state that one should always respond providing all data always, the language is ambiguous and seems to encourage sending more or all data, including reaching out to all QHINs rather than those most likely to have eHI, for the patient at hand.

Recommendations:
We suggest that ONC clarify that data requests should be, as much as possible, focused on minimum necessary, which may include all data for a particular purpose. Particularly with the introduction of data element level queries, we have the opportunity to optimize access and exchange thus not unnecessarily driving up costs to accommodate sending everything always. To optimize access and exchange across QHINs, we suggest that QHINs be able to share record location information through ADT/Event notifications that enable the requester to better target their requests.

Data Quality Characteristics

Concern/Question:
The section on Data Quality Characteristics indicates the responsibility of the RCE to perform regular data quality evaluations with the QHINs. This does not address QHIN participants (holders and sources of the demographic data) nor the expected follow-up.

Recommendations:
We suggest that the evaluation extend to the QHIN participants and that the RCE uses the results to identify opportunities for improvement to address in the next round of capability planning, thus creating a closed loop learning system.

Population Level Queries

Concern/Question:
We appreciate and support the need to access and exchange data in support of various population level use cases. We are concerned that the proposed capabilities are not necessarily mature and/or well-suited to obtain such data. We refer to our comments on Modular and Optional Capabilities for how this can be addressed.

Additionally, it appears that Part B, Section 8, implies that obtaining such data can be based on "fuzzy" query parameters, e.g., patients older than 18 with a diagnosis of congestive heart failure in select zip codes. We note that the text gives a different impression than the explanations in the webinars that a query is based on a specific patient list. Additionally, the expected response times are suggested to be less than 24 hours, which depending on the query and other competing requests may or may not be reasonable.

Recommendations:
We suggest clarifying that queries must be based on a defined set of patients for whom clear authorization and consent is provided rather than indeterminate, "fuzzy" queries. We note that for certain permitted purposes outside of Treatment or Payment, consent management for large queries is challenging and not yet established, requiring further definition. Clarity is needed on how either the requester can communicate this and the receiver should consider the consents provided.

We suggest that expectations on response times to large queries not be established until adequate experience demonstrates the duration of reasonable response times. Such expectations should then be included in the RCE implementation compendium for the applicable use cases and are an example of where transaction prioritization and frequencies could be applied.

Consent Management

Concern:
Consent management for dynamic data queries has not yet been clearly defined, in particular how specific consent around sensitive data, 42 C.F.R. Part II, re-disclosures, or self-pay related data can be best managed when part of larger dataset queries.

Recommendations:
We suggest that consent management requires further definition through implementation guidance and pilot testing before it is ready to be widely applied beyond general consent management constructs.

Privacy and Security

Concerns:
Overall, the Trusted Exchange Framework aligns with our position in support of the development of mechanisms, technical standards, and policy changes that promote and provide nationwide, standards-based interoperability framework for access, disclosure and exchange of Protected Health Information (PHI) built on agreed-upon security and privacy principles.

We appreciate that TEFCA has attempted to align with HIPAA. However, we are concerned that the aggressive timeframe for implementation may increase the risk of privacy and security issues, as HINs will not have proper time to test the trusted framework prior to implementation.

Recommendations:
We request clarity regarding some of the permitted purposes. Specifically, what is encompassed in "Benefits Determination," as there are some benefits determination scenarios that may not be under Treatment, Payment, and Operations (TPO) under HIPAA?

6.1.3. Regarding Breach notification, we are not clear on whether this is limited to breaches at the QHIN level, or if this breach notification requirement extends to the participants of the QHIN. In cases where the participants or the QHIN are subject to multiple breach notification clauses, the Trusted Exchange Framework should provide one breach notification channel.

6.1.6. In its current form, the Trusted Exchange Framework lacks guidance on standards on Patient Consent. 45 C.F.R. has very clear guidelines on standards for informed consent; TEFCA should detail a similar standard specific to this use case. In addition, the draft does not address how to reconcile possible conflicting consent across multiple sites. Is consent treated as HIN-specific, or is there an

expectation that patient consent is holistic in the health system? We recommend a centralized and holistic healthcare industry patient consent model, rather than site-specific patient consent.

6.1.6 Patient Matching. How do stricter regulations, such as 42 C.F.R. Part 2, and their restrictions on sharing data fit the "permitted purposes" clause of TEFCA?

6.2.1 We agree with aligning the Trusted Exchange Framework requirements around the NIST cybersecurity framework. EHRA recommends that our members implement a cybersecurity framework based on the NIST framework.

6.2.2. For Data Integrity, this requirement can be achieved at the message level or the transport level. If at the transport level, the requirement should be to use Transport Layer Security (TLS). If at the message level, the requirement should be that it is done over a secure channel.

6.2.4. Though we agree with the need for Identity Proofing, the need for Identity Assurance Level 2 (IAL2) at the end-user and individual level may create a barrier to the adoption of this program, as this requirement is onerous. Some identity proofing of the participant makes sense, but there should be a way for participants to vouch for their members. We believe participants should make a reasonable effort to identity proof an end-user or an individual.

6.2.5. When accessing the system, for some TEFCA stakeholders, there are care implications that must be considered with authentication. Authentication for a user in a healthcare setting is a multi-faceted approach with a combination of physical security, trusted devices, etc. We need to be flexible and be careful not to introduce undue burden to the user.

Transport Security

Recommendations:

6.2.7.i.b. We are strongly against the reference to null, substitution, and transposition ciphers; they are outdated and should not be used. The Trusted Exchange Framework should instead make a reference to use TLS exclusively to achieve transport security.

6.2.7.i.c. Message exchange security should support TLS 1.2 wherever possible and a minimum of TLS 1.1 only for compatibility of older systems. We recommend the removal of any mention of Secure Sockets Layer (SSL).

6.2.7.ii.a - A dynamic client registration is a potential security risk and the authorization server should be allowed to only establish trusted relationships. This should not be perceived as information blocking, but as a security risk abatement practice.

6.2.7.2.b - Authentication Server Requirements for Third Party should have a commonly accepted token assertion in the industry, without the mention of JSON. We are not questioning JSON; however, we do not want to specify a token format that may become obsolete in the future.

6.2.7.iii.c - The decision to refresh tokens or not should be solely with the authorization server, based on the client profile.

6.2.10 - Regarding Auditable Events, the Meaningful Use (2015 Edition Certification Criteria) requirement for auditing should be referenced.

6.2.12 - We request clarification on whether IP Whitelisting is intended for only server (QHIN) to server (QHIN) communication. If not, then IP Whitelisting (6.2.12) should be done based on a risk assessment and should not be a mandatory requirement because not all devices can be subject to IP Whitelisting, such as a mobile device where the IP address is dynamic. In addition, any IP address whitelist directories must be secured (only accessible to those in the trusted exchange), as this list can be a tool used by malicious adversaries to compromise security.

We welcome the Trusted Exchange Framework's approach to be more prescriptive in the "minimum requirement" section, including referencing the latest NIST publications, such as 800-63, which EHRA has encouraged. While the mention of explicit protocol/standards certainly helps from an implementation perspective, there is the risk of a standard or protocol becoming weak, especially in the case of cryptography, where the strength of an algorithm is often based on the mathematical and computational complexity, which is constantly challenged due to advancements in computational resources and power.

In that regard, we ask that where the document makes a reference to a specific standard or protocol, it prefixes that with "at least," which leaves room for a more secure algorithm/standard to be implemented, or references an external publication such as FIPS/NIST.

EHRA strongly supports efforts to improve interoperability and expand access to data as a means of improving delivery of high-quality healthcare. In support of this goal, we frequently collaborate with data exchange networks, including CareQuality, CommonWell, and eHealth Exchange. We believe the TEFCA has the potential to dramatically improve interoperability, however we recommend ONC look to leverage existing investments in interoperability and build upon these successes with close stakeholder collaboration.

We look forward to working with ONC and the Recognized Coordinating Entity to build upon current interoperability infrastructure and drive continued progress toward nationwide interoperability.

Sincerely,

Sasha TerMaat
Chair, EHR Association
Epic

Cherie Holmes-Henry
Vice Chair, EHR Association
NextGen Healthcare

HIMSS EHR Association Executive Committee

Hans J. Buitendijk
Cerner Corporation

Nadeem Dhanani, MD, MPH
Modernizing Medicine

David Heller
Greenway Health

Rick Reeves, RPh
Evident

About the EHR Association

Established in 2004, the Electronic Health Record (EHR) Association is comprised of more than 30 companies that supply the vast majority of EHRs to physicians' practices and hospitals across the United States. The EHR Association operates on the premise that the rapid, widespread adoption of EHRs will help improve the quality of patient care as well as the productivity and sustainability of the healthcare system as a key enabler of healthcare transformation. The EHR Association and its members are committed to supporting safe healthcare delivery, fostering continued innovation, and operating with high integrity in the market for our users and their patients and families.

The EHR Association is a partner of HIMSS. For more information, visit www.ehra.org.