233 N. Michigan Ave.,21st Fl.
Chicago, IL 60601-5800

phone » (312) 233-1100
fax » (312) 233-1090
web » www.ahima.org

AHIMA
American Health Information Management Association®

February 20, 2018

Dr. Donald Rucker
National Coordinator
Office of the National Coordinator for Health Information Technology
330 C Street, SW
Floor 7, Switzer Building
Washington, DC 20024

Dear Dr. Rucker:

Thank you for the opportunity to provide comments on the draft Trusted Exchange Framework.

The American Health Information Management Association (AHIMA) is the national non-profit association of health information management (HIM) professionals. Serving 52 affiliated component state associations including the District of Columbia and Puerto Rico, AHIMA represents over 103,000 health information management professionals dedicated to effective health information management, information governance, and applied informatics. AHIMA's credentialed and certified HIM members can be found in more than 40 different employer settings in 120 different job functions—consistently ensuring that health information is accurate, timely, complete, and available to patients and providers. AHIMA provides leadership through education and workforce development, as well as thought leadership in continuing HIM research and applied management for health information analytics.

Although the draft Trusted Exchange Framework addresses a myriad of topics, we would like to offer below some general comments about the Framework, followed by more specific comments.

General Comments

Alignment with HIPAA

AHIMA supports ONC's intent to align the draft Framework with HIPAA requirements to the extent possible. Such alignment will not only serve to reduce confusion by qualified health information networks (HINs) and participants but serve as a deterrent to the creation of artificial barriers when exchanging electronic health information.

Sustainability of the Recognized Coordinating Entity

AHIMA agrees with ONC that an industry-based recognized coordinating entity (RCE) is perhaps best positioned to operationalize the Framework considering the proposed cuts to ONC's budget by the current Administration. However, we are concerned about the long-term sustainability of the RCE. While we understand that the cooperative agreement is intended to be a multi-year agreement, we are concerned that if the Trusted Exchange Framework and Common Agreement (TEFCA) is not intended to be released until late 2018 and qualified HINs have at least 12 months from the date of publication of the final Common Agreement to update their participant agreements to incorporate the terms and

conditions set forth in the TEFCA, that could offer little inducement for HINs to participate in the TEFCA if there is uncertainty around future of the RCE itself.

Applicability of State Law under the TEFCA

AHIMA is concerned that the draft Framework lacks sufficient clarity on the applicability of state law when responding to a query/pull. While we understand that the Framework is not intended to be all-encompassing with respect to terms and conditions and that the Common Agreement is intended to incorporate additional, more specific provisions related to the exchange of electronic health information, we are concerned that the Framework does not make clear the applicability of state law when exchanging such data. For example, in responding to a query/pull, will a qualified HIN be responsible for sending data that in accordance with its own state law or will it be required to send data according to the initiating qualified HIN's state law? We suggest that the Framework and/or the Common Agreement provide further discussion around the implication of state laws vis à vis the Framework in terms of the types electronic health information that may be requested and exchanged.

Detailed Comments

Part A – Principles for Trusted Exchange

Principle 1 – Standardization

AHIMA appreciates that the Framework calls for adherence to federally adopted or recognized standards for electronic health information. We agree with ONC that at a minimum, qualified HINs should adopt and use standards and implementation specifications referenced in the 2015 Edition final rule and the Interoperability Standard Advisory (ISA). That said, we are concerned about whether certain standards may be mature enough and sufficiently piloted in the field to merit adherence and adoption. For instance, the data classes cited on page 6 of the Draft U.S. Core Data for Interoperability (USCDI) Version 1 do not point to specific standards and instead some have multiple standards listed under each category of the ISA. It is unclear from the Framework and the USCDI which standards must be used together to meet interoperability needs. For example, there is not a standard for the patient name in terms of collecting the name in the same form and format to facilitate patient matching. Additionally, with respect to laboratory values/results, although LOINC® is a fairly mature standard for lab results, feedback is still requested under the 2018 Interoperability Standards Advisory (ISA) for SNOMED CT®. It is not clear from the draft Framework whether one or the other will be recommended and/or mandated. It is also not apparent from the Framework or the USCDI whether the Units of Measure will be required to meet this standard in conjunction with LOINC or SNOMED CT.

Principle 2 – Transparency: Conduct All Exchange Openly and Transparently

AHIMA supports the requirement under the Framework that a qualified HIN must publish, keep current and make publicly available its privacy practices. This is important since a qualified HIN can be a business associate which is not required to create a notice of privacy practices under HIPAA. We believe this requirement will assist in providing further transparency to a qualified HIN's privacy practices.

Principle 4 – Privacy, Security, and Patient Safety

AHIMA recommends that Principle 4 include the following language: "Exchange Electronic Health Information securely and in a manner that promotes patient safety, ensures data integrity *and adheres to privacy policies."* This technical change highlights the critical privacy-related requirements in subprinciple (B) and is distinct from the subprinciples related to patient safety and data integrity.

Principle 5 – Access

AHIMA is pleased that ensuring that individuals have access to their electronic health information without special effort is a principle of the draft Framework. As a member of the GetMyHealthData campaign, AHIMA has long advocated that a consumer's access to his or her health information is essential to improving health and healthcare. We continue to support efforts that improve the ability of a consumer to access his or her health information.

We appreciate that the draft Framework requires qualified HINs and their participants to not limit third-party applications from accessing an individual's electronic health information via an API when the application complies with the Framework's requirements and is directed by the individual. We believe this requirement may provide some initial guardrails for HIM professionals within their institutions who are challenged to manage such requests when the third-party application is not necessarily a covered entity or business associate but the institution must comply with the patient access request under HIPAA.

AHIMA also supports the inclusion of policies and procedures that would allow a patient to withdraw or revoke his or her participation in a qualified HIN. However, it is unclear from the Framework whether a patient would necessarily know which qualified HIN(s) they participate in to be able to revoke their consent. Additionally, would a patient's withdrawal from a qualified HIN be sufficient to revoke participation in other qualified HINs that may hold some of the patient's electronic health information? How would notification to other qualified HINs and/or participants work when a patient decides to revoke their participation? Would the RCE need to be notified of the patient's revocation? We understand that the Common Agreement may address some of these requirements, however, we want to ensure that in the event a patient decides to revoke their participation in a qualified HIN, the information remains protected and undisclosed.

Part B – Minimum Required Terms and Conditions for Trusted Exchange

1.Definitions

AHIMA supports the permitted purposes articulated in the draft Framework. However, we believe that ONC should consider research as a permitted purpose, which could enable researchers to have access to de-identified health information. The availability of the data could in turn be used to conduct research to help identify factors and useful information to improve healthcare delivery. For example, researchers submitting a request to access this data could be identified using a unique identifier of alphanumeric value after validating the individual's credentials. The aforementioned data could then be provided on the condition that the results of the research be made available by means of publication, which would be made publicly available by ONC.

3.Standardization

AHIMA supports the requirement under "3.3: Patient Demographic Data for Matching." Section 3.3 will help to establish a floor in the exchange of certain data attributes and the standardizing of such data. However, we are concerned that the requirements may not be enough to accurately identify a patient and could result, particularly in the execution of a broadcast query, in multiple records being returned, thereby requiring a back-end reconciliation process. Compounding this problem is the fact that participants may have policies and procedures that vary in terms of how the data attributes are entered into the system to begin with. For example, differences may arise in data collection with respect to legal name versus nickname (e.g.—Elizabeth Smith versus Betty Smith), hyphenated names or names with special characters, and/or differentiations in addresses (e.g.—111 Crane Trail versus 111 Crane Trl).

It is unclear from the draft Framework whether the qualified HIN or the participant would be responsible for the reconciliation and whether the Framework and/or Common Agreement encourages the parties involved to work toward more standardized methods of collecting patient matching data. Furthermore, AHIMA is concerned about instances where electronic health information is sent to an initiating qualified HIN and despite using the data attributes required in 3.3, the wrong patient's information is sent. Under such a scenario, it is unclear under the Framework how the information may be retrieved by the qualified HIN and/or whether the responding qualified HIN should be notified or alerted that incorrect information was shared.

We request that ONC provide further clarification around which party would be responsible for reconciling multiple records. We also suggest that under 3.3, the Framework require, **at a minimum**, that a qualified HIN support the exchange of patient matching data enumerated in the 2015 Edition certification criterion. We believe that this small, technical change could encourage qualified HINs and participants over time to collect, maintain, standardize, and exchange additional data attributes that could improve patient matching. Additionally, we also suggest that ONC consider including some of the recommendations set forth in "Health IT Safe Practices: Toolkit for the Safe Use of Health IT for Patient Identification" as part of the Framework. Finally, we also request that ONC provide further clarity on how qualified HINs should remedy situations where incorrect electronic health information is sent.

AHIMA also supports the requirement under "3.4: Data Quality Characteristics" requiring qualified HINs to evaluate their patient demographic data management practices using the ONC Patient Demographic Data Quality (PDDQ) Framework. AHIMA supports an enterprise wide information governance approach to patient identity, including, but not limited to the data governance approach described in the PDDQ Framework. AHIMA views data governance as a sub-domain of information governance, which provides for the design and execution of data needs, planning, and data quality assurance in concert with the strategic information needs of the organization.

6. Privacy, Security, and Patient Safety

AHIMA agrees with the requirements under "6.1.6: Consent" and "6.1.7: Revocation of Consent" in the Framework. However, we are concerned about situations where the electronic health information is contained in an integrated health record and includes substance abuse disorder and treatment information covered by 42 CFR Part 2. It is unclear according to the Framework whether an individual could revoke their consent for information covered by 42 CFR Part 2 or whether the consent must apply to all the individual's electronic health information. We recognize that not all vendor technologies are mature enough to be able to segment such sensitive data and that it is often the case that to protect

such sensitive information, HIM professionals must create a second record that contains only Part 2 information. However, as integrated care delivery models continue to be implemented, we believe that the Framework, Common Agreement and/or participant agreements should contemplate at some point the ability to provide such granular consent.

Furthermore, we are also concerned that SAMHSA's Final Rule issued in January 2018 adds an additional layer of complexity to the Framework by allowing lawful holders to re-disclose substance abuse disorder records as may be necessary to contractors, subcontractors, or legal representatives to carry out payment and/or healthcare operations on behalf of the legal holder but not for treatment purposes. Assuming the qualified HIN is considered a subcontractor or contractor to the participant, this limitation could inhibit the exchange of electronic health information given that treatment is a permitted purpose under the Framework.

We understand that these concerns might be beyond the scope of ONC's authority, however, we do believe that the explicit authorizations required under Part 2 could make it difficult to share electronic health information as envisioned by the TEFCA. Therefore, we respectfully request that ONC work with SAMHSA to provide greater clarity on these issues.

AHIMA also recommends that whether it be under "6.1.7: Revocation of Consent" or in the Common Agreement that the policies and procedures required to be maintained by the qualified HIN make clear that should a qualified HIN be a covered entity, it is not required under HIPAA to agree to restrict protected information (PHI) unless it is in accordance with 45 CFR 164.522(a)(1)(vi). Our members have expressed concern that 6.1.7 appears to indicate that an individual may unilaterally revoke their permission to use and disclose their electronic health information. However, should the qualified HIN be a covered entity under HIPAA, the covered entity would not be required to restrict the use and disclosure of the PHI except as provided in 45 CFR 164.522(a)(1)(vi).

Additionally, under "6.2.4: Identity Proofing," it is somewhat unclear with respect to the task of identity proofing an individual whether the qualified HIN is charged with identity proofing the individual or the participant or end user. In contrast, page 25 of the User Guide makes clear that a qualified HIN must require its end users and participants to proof the identity of individuals. We recommend that a similar clarification be made in the Framework to avoid confusion.

AHIMA supports the inclusion of a "trusted referee" acting as an authoritative source of the individual's identity which could provide much-needed flexibility when individuals lack the necessary identity evidence needed to meet the requirements of IAL2 under 6.2.4. That said, to ensure that the trusted referee is properly trained to accurately identify an individual, we recommend that the trusted referee be a person with a validated skill set trained in identity management such as an HIM professional.

9. Participant Obligations

Under "9.1.6: Security Incident and Breach Notification Requirements," it is unclear whether participants that are not covered entities or business associates must comply with the notification requirements to a qualified HIN in the event of a discovery of a breach. We recommend that ONC clarify whether such a notification will be required of all participants, because if such entities are not required to comply with the breach notification requirements under HIPAA, at a minimum they should be required to report a breach to a qualified HIN to ensure that other participants affected by the breach are made aware. We believe similar ambiguity exists in "10.1.5: Security Incident and Breach

Notification Requirements" with respect to the end user and that ONC should provide further clarification.

We appreciate the opportunity to submit comments on the draft Trusted Exchange Framework. We hope that you will continue to engage extensively with stakeholders on the Framework and we look forward to working with you to ensure its successful final release and implementation.

Should you or your staff have any additional questions or comments, please contact Lauren Riplinger, Senior Director, Federal Relations, at lauren.riplinger@ahima.org and (202) 839-1218.

Sincerely,

Dr. Wylecia Wiggs Harris, PhD
Chief Executive Officer
AHIMA