June 17, 2019

Don Rucker, M.D.
Office of the National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
330 C Street, SW
Washington, DC 20201

Dr. Rucker:

I am pleased to submit Allscripts' comments to the Office of the National Coordinator for Health Information Technology on the *Trusted Exchange Framework and Common Agreement (TEFCA) Draft 2*. With a platform of clinical, business and interoperability solutions for ambulatory, acute and post-acute settings, we are relied upon by the industry's largest network of providers – over 330,000 physicians in more than 70,000 different practice locations, almost 2,400 hospitals and more than 100,000 post-acute care providers. It is through our three decades of experience partnering with and deploying software to this vast network of providers that we can submit informed comments today on this important topic.

General Comments

We applaud ONC for continuing to refine the requirements to advance interoperability across the healthcare ecosystem. Since our involvement with the legislative development effort, Allscripts has supported the intent and goals of the 21st Century Cures Act to enable nationwide data access and exchange in order to more effectively coordinate patient care and facilitate research. For almost twenty years, we have supported our clients in participation with a wide range of exchange efforts, including point-to-point through our HIE solution (dbMotion), open API-based exchange since 2007, and DIRECT. We are currently in process of connecting our EHRs to the Carequality network, as well.

This second draft of TEFCA guidance increases the clarity of the proposed approach in many areas, and we appreciate that several big thematic issues raised with Draft 1 have been addressed. However, there are still challenging questions and the need for several points of clarification. In particular, the concepts released go well beyond what was intended by Congress, which was a framework to address governance and trust issues that were impeding information flow, as well as an accompanying template for contract language that might help people avoid spending unnecessary time or money on the legal arrangements inherent to information exchange (particularly related to payment models such as ACOs, or where concerns about privacy and security were raised). Instead, ONC has included elements in the TEFCA Draft 2 that are far outside those constructs, including addressing technical elements, whole new concepts for industry classification, and approaches that may not find strong market interest among those – providers – who will need to be the ones to participate.

Because so many new concepts are proposed and they are done so in a way that would require replacement of initiatives already underway, we have concerns about how the proposal would enable continued growth and support of existing private-sector exchange efforts. Networks established in different regions have come a long way over the last

decade, having successfully addressed how to exchange data and learning a great deal about which types of data offer the most value to healthcare providers and patients when exchanged. Allscripts, for example, supports over 80 million patient lives through our dbMotion solution, and the networks that have been built in that process would be disrupted at the cost of patient care if they were to have to step back from what is already working. What is proposed in TEFCA Draft 2 appears to be almost a parallel new framework rather than one that would build on established networks and processes like those described above.

Further, we note that Congress intended for TEFCA to be a voluntary, non-prescriptive source of assistance to the industry in grappling with a few challenges to information exchange. However, through elements of TEFCA Draft 2, the likely possibility of other HHS programs pointing to TEFCA participation as a requirement, and mentions in the Information Blocking NPRM about possible mandatory participation, we believe this essentially lays the groundwork for TEFCA participation to not, in fact, be voluntary. Voluntary programs can reasonably be more challenging or set a higher bar because stakeholders have the option not to agree to those more demanding requirements; if a program is to be mandatory and thus involve companies and provider organizations from the smallest to the largest, the threshold for participation can only be expected to be easier to achieve. The fact that the bar is high, the prescriptivity is significant and the voluntary element is not, in fact, voluntary, is a mismatch in the TEFCA Draft 2 approach.

We agree with ONC that nationwide scalability is needed to optimize interoperability. TEFCA should provide the base requirements to enable developers and others to join and participate. The minimum requirements should guarantee entry into TEFCA and allow for entities to achieve higher standards if they choose to do so. The minimum and optional standards should be given time to evolve with industry collaboration, as this will allow room for growth and innovation. As stated above, TEFCA should build upon existing infrastructure and requirements, such that necessary rework is minimal.

We also highly encourage attention be given to the data input workflow. Much of the current framework draft includes outflow examples (e.g., EHI Export), and does not set standards or dictate how a system should receive the information. Accounting for data input is vital to the success of TEFCA. For example, this effort is focused on accessing the data, however this is half of the equation when discussing the functions of HIEs and HINs. The other half of the solution will require health systems to become repositories to store and use the data, and that should be addressed in future versions of TEFCA documents.

Security is a fundamental requirement to trusted data exchange. Throughout the comments below, we highlight where there would be impacts on system security and offer options and solutions. We ask that the final version of TEFCA address how security will persist throughout the system. There are various requirements, however, we would like to see security continuity be addressed. For example, more details are needed around authorization and consent. Additionally, there should be end-to-end authorization, federation of disparate systems, and access control that spans all QHINs.

The Trusted Exchange Framework (TEF)

Allscripts supports the principles underlying the TEF concepts. Increasing standardization across the industry will be an important driver to successfully expanding information exchange. While Allscripts and others in the industry raised significant concerns with many of the proposals in the Information Blocking NPRM, we do appreciate attempts within

both to complement and consistently approach key topics across both. We also request that ONC consider where participation in TEFCA can alleviate vendors and other entities from certain certification requirements, rhetorically speaking, should TEFCA serve as a cost-savings opportunity for both ONC and vendors.

We appreciate and support many of the basic principles outlined and described; in many cases, these principles are already in place in existing networks or national frameworks such as Carequality, and it will be important that ONC use the next draft of the TEFCA documents to reinforce but not unnecessarily duplicate what is already working. We do suggest that ONC and the proposed RCE work with stakeholders to identify key metrics that measure success toward the goals of a trusted exchange framework (e.g., number of connected endpoints per use case, number of transactions by type, time to connect to "all") and adherence to its principles.

Principle 1 *— Standardization: Adhere to industry and federally recognized technical standards, policies, best practices, and procedures.*

We applaud ONC for continuing to work towards adoption and use of consistent standards through the 2015 Certification program and the 21st Century Cures Act proposed rule. In addition to setting standards for the industry to use, it is equally important for ONC to develop and maintain standardized tools. Enabling each HIN/QHIN to construct their own tools would create an implementation quagmire and absolutely result in an unintended consequence of slowing down interoperability and increasing the cost of participation in TEFCA. For example, if each HIN or QHIN were to create their own tools, there is the potential for issues to occur between networks; we see this now between HIEs. Further, when we as software development vendors have to do custom work specific to each different network, it means our clients see unnecessary cost passed to them. Conversely, standardized, centralized tools would positively affect the rollout and maintenance of TEFCA.

Principle 2 *— Transparency: Conduct all exchange and operations openly and transparently.*

Principle 2 complements the prohibition of information blocking well. It is important that everyone be held to this standard such that vendors supporting multiple systems nationally are all treated the same, whether they participate in TEFCA or not.

Principle 3 *— Cooperation and Non-Discrimination: Collaborate with stakeholders across the continuum of care to exchange EHI, even when a stakeholder may be a business competitor.*

Principal 3 also complements the information blocking proposed rule, although it does not specifically mention it. We support and encourage ONC to incorporate the same language that is forthcoming in the 21st Century Cures Information Blocking final rule in the final version of TEFCA so the expectations are clear and consistent, and there is no ambiguity when interpreting the applicable requirements. We agree all entities must treat each other the same, however not all entities *are* the same; for example, responding to an individual patient request will be different from responding to a health system inquiry. Perhaps there needs to be a consumer-facing QHIN that is promoted for individuals to access.

Principle 4 *— Privacy, Security, and Safety: Exchange EHI securely and in a manner that promotes patient safety, ensures data integrity, and adheres to privacy policies.*

Promoting privacy, security and safety are of the upmost importance to Allscripts. We support this principle, as it is foundational to effective data exchange. It is important that any future versions of TEFCA include a much more detailed focus on how security will persist throughout the newly-expanding exchange ecosystem. Additionally, we encourage ONC to continue focusing on the promotion of patient matching guidance that is practical across HINs (and applicable to access by other data consumers) in order to do whatever is possible to implement consistent and reliable business rules that will result in accurate patient data from location to location.

Principle 5 *– Access: Ensure that Individuals and their authorized caregivers have easy access to their EHI.*

It is important to balance the need for security, such as ID proofing, with the practicality of individual consumers completing it. Ensuring data security is essential; however, we are concerned that if the process is too cumbersome, individuals will access their data through other means, such as consumer apps that do not require the same level of ID proofing, and in turn may not be as secure. Thought should be given to making the ID process easy, and HHS should invest in educating the public about the importance of safeguarding that informatoin.

Principle 6 *— Population-Level Data: Exchange multiple records for a cohort of individuals at one time in accordance with applicable law to enable identification and trending of data to lower the cost of care and improve the health of the population.*

Allscripts is supportive of Principle 6. Allowing the exchange of multiple records for a cohort of individuals at one time will improve efficiency of data exchange, and in turn improve patient care.

Minimum Required Terms & conditions (MRTCs)

QHIN Operations

It is, of course, important to comply with all applicable laws, both federal and state. However, HIEs, HINs and QHINs will each be inclined to implement their own contract language in addition to all applicable local and Federal laws. Currently, disparities between those contracts result in delays negotiating contract requirements between different networks. Therefore, we request ONC provide clarification on various restrictions (which laws overrides which others) and how any confusion or conflicting laws will be resolved. It would be advantageous to the industry for TEFCA to provide the baseline, allowing HINs and QHINs to then add additional rules within their contracts that do not restrict the TEFCA baseline.

QHIN Operations: Termination of Participation in the Common Agreement

We are supportive of the option for a QHIN to be terminated from participating in the common agreement, however we are concerned about the management of any related process. What controls will be in place for those who are terminated, or those to voluntarily drop out? How will continuity of data exchange be guaranteed? How will termination or voluntary dissolution be communicated to others participating in TEFCA? Moreover, will a QHIN have the responsibility and capacity to drop Participants deemed to be bad players not contributing or violating rules? The same

questions apply to individuals (patients), so we request clarification and examples in the next iteration of guidance on the CA.

QHIN Operations: Transparency

Allscripts recommends that a requirement be added to the transparency section to post HIN and QHIN contact information publicly. Like the proposal to post all Direct addresses publicly that was included in the CMS interoperability rule, requiring all HINs and QHINs to post contact information publicly will make participation easier and more efficient.

Privacy, Security, and Data Integrity: Data Integrity

We disagree that the QHIN should be responsible for reporting inaccurate or incomplete EHI to the Participant who is the originator of the EHI. This seems an unreasonable and burdensome expectation. If the QHIN notices a data issue, then yes, they should report it; however, the entity where the data was originally collected is responsible for that data and should be held accountable for ensuring its integrity. They should correct inaccuracies and update the QHIN to ensure consistent and correct data is available.

Also, we have a question about this statement on page 19, located under the Security Labeling header: "Labeling shall occur at the highest (document or security header) level". We agree discrete data must be labeled. Does this imply the document, bundle, or container for that labeled date must be labeled to match the level of the most restriped discrete data, or does labeling refer to the human readable notification to the user? We caution that processing data within an application with privacy and security permutations is complicated, and the more variations, the greater the complexity and risk to the data. We suggest that there needs to be deeper and more thorough addressing of this topic going forward.

Privacy, Security, and Data Integrity: ID Proofing

ID proofing is an important step to securing data. Allscripts recommends that TEFCA not define its own standard, or a variation of a standard. We support the proposal in this draft to use IAL 2 described in NIST Special Publication 800-63 (Revision 3), Digital Identity Guidelines (June 2017). This standard should be used universally across QHINs; once an individual has completed ID proofing, it should be transferable.

Last, we encourage ONC to consider how to verify machines' (and turn, systems') identities. For example, ONC should consider requiring the use of public trust certificates for machine verification.

Participant Minimum Obligations: Breach Notification Requirements and Security Incident.

It is important to have clear protocols in place in the event of a data breech. If a Participant learns of a data breech, we recommend they be required to notify the QHIN, who has access to all the Participants, Participant Members, and Individuals. QHINs are in the best position to distribute information to all affected, or potentially affected, entities.

Participant Minimum Obligations: Data Integrity

We feel strongly that the entity who created the data should be responsibility for its accuracy. Participants will aid in moving data, however they will clearly not always also be the originator. For example, an IT vendor who serves as a Participant provides clinicians with a tool to record and store data but is not able to verify its accuracy. We also must express concern about Patients being able to correct their own data, too. Patients should be able to (easily) access and view their health data so that they can notify a clinician of any issue they may notice. However, giving a patient the access to alter a medical record without that action being monitored and tracked in some way, as well as validated by a clinician, poses real risk to value of that data going forward and could directly affect their care.

Qualified Health Information Network (QHIN) Technical Framework Requests for Comment

ONC Request for Comment #1: *Should the QTF specify additional standards or approaches for securing QHIN Exchange Network transactions (e.g. OASIS Web Services Security47)?*

ONC should establish baseline entry standards, such as requiring a common CA or trust bundle from Direct Trust for securing QHIN Exchange Network transactions; doing this will ease implementation issues, speed implementation exchange, and provide consistency for Participants as they onboard.

ONC Request for Comment #2: *What specific elements should a SAML assertion for User Authentication include?*

We don't have specific recommendations about what elements a SAML assertion should include; however, we do ask that whatever is decided is properly vetted by the industry before being finalized as a requirement. We do recommend choosing a method that can handle automated responses, such as the NHIH authorization Framework v3.

ONC Request for Comment #3: *Should QHINs be required to transmit other authorization information (e.g., user roles, security labels) in addition to Exchange Purpose and any information required by IHE XUA? What specific elements should a SAML assertion include?*

We agree with the idea of transmitting authorization information, such as user roles and security labels, but there needs to be a national standard set first, such as OAuth. Currently, the authorization definitions vary across vendors, and business models and mapping would be necessary to make the data meaningful. Another possible solution outside of Setting a mandatory standard is for there to be a discrete list of actions end users can perform, which would then allow vendors to map their authorization levels to those parameters.

ONC Request for Comment #4: *The Query function above describes a general workflow and set of capabilities for QHINs conducting query-based, inter-network document exchange. However, implementations may vary and result in divergence from the basic workflow. For example, a QHIN might fail to definitively resolve patient identity and consequently rely on a participant or Participant Member to determine the correct match. Likewise, Carequality's Query-Based Document Exchange Implementation Guide49 describes a number of alternate flows based on a "nominal flow." To inform subsequent work with the RCE to develop more specific technical guidance to address variation, comments are requested on the basic function presented and potential variations to consider.*

We recommend ONC establish a ground floor entry level set of workflows that must be minimally supported by someone to quality as a Participant. Once the baseline is set, ONC should allow for use cases to influence it with the goal of future evolution. If ONC is overly prescriptive when it comes to this area – determining workflows, for example – it could have a limiting effect on innovation advancements across the industry.

ONC Request for Comment #5: *The IHE XCA profile supports a number of defined queries (e.g., FindDocuments, GetAll, GetDocuments, GetRelatedDocuments, etc.). Each query includes a number of optional parameters. Should the QTF specify which queries/parameters a QHIN must support? Which queries/parameters are most widely implemented and/or useful today?*

We recommend ONC define a minimum set of queries vendors must perform, as well as additional queries that are optional. Furthermore, we request ONC not restrict functionality, though we believe it appropriate for ONC to define what error should be returned for each query, so vendors can respond even if they do not have the functionality. This will allow room to grow without having to agree on updated specifications or make modifications to adopt a new query or stop using one – the protocol would already be established.

ONC Request for Comment #6: *The IHE XCA profile is content-agnostic; it enables queries for documents based on metadata about the document but not the contents of the document itself. Therefore, the XCA profile does not necessarily support more granular queries for discrete data (e.g., a request for all clinical documents about a patient that contain a specific medication or laboratory result). Comments are requested on other appropriate standards to consider for implementation to enable more discrete data queries, such as emerging IHE profiles leveraging RESTful APIs and/or use of HL7 FHIR.*

Allscripts recommends ONC establish a minimum entry level for documents that are XML-based. For queries specific to FHIR, the standards should be consistent with the forthcoming ONC Information Blocking Final Rule. We also recommend ONC create a central framework or tool to validate events like what was used for Meaningful Use 3 to validate Transition of Care transactions.

ONC Request for Comment #7: *The IHE XCPD profile only requires a minimal set of demographic information (i.e., name and birth date/time). Should QHINs use a broader set of specified patient demographic elements to resolve patient identity? What elements should comprise such a set?*

Allscripts agrees QHIN's should use a broader set of specified patient demographic elements to resolve patient identity. The elements should include:

Last Name
First Name
Date of Birth (Year)
Date of Birth (Month)
Date of Birth (Day)
Birth Time
Gender (Administrative)

SSN (Not frequently transmitted)
Current Address
Birthplace Address
Birthplace Name (i.e. Hospital Name)
Mother's maiden Name
Email
Phone (cell)
Medicare number/ID

ONC Request for Comment #8: *There are many possible approaches to Patient Identity Resolution, each with its own benefits and risks. For example, a centralized index of patient identity information may be more efficient for resolving patient identities across disparate communities, but also poses a greater risk to privacy if the system is compromised. Federated approaches may be less susceptible to external threats like cyberattacks, but harder to scale across many communities. Recognizing that new technologies and business entities with robust identity matching solutions may disrupt traditional approaches, should the QTF specify a single standardized approach to Patient Identity Resolution across QHINs?*

Allscripts recommends a single, standardized, centralized system, or that a common algorithm be established. This would reduce burden and time to process transactions. We do not foresee this adding an additional security risk because patients still must be matched. In fact, when patient identification is more complicated or requires more steps and/or resources (e.g. computers and humans), there is actually more room for error. Adopting a consistent algorithm would help ameliorate that risk.

ONC Request for Comment #9: *Different communities tolerate different degrees of risk with respect to accurately matching patient identities. Should QHINs meet a minimum performance standard (e.g., a minimum acceptable matching accuracy rate) over a specified time period? Likewise, different algorithmic techniques for matching patient identities use different approaches and must be tuned to the applicable patient population and continuously refined over time. Should QHINs measure and report on the performance of the algorithm(s) they rely on (e.g., by calculating precision, recall, etc.)?*

Allscripts agrees that creating a consistent and measurable process with dependable monitoring is ideal, but comparing QHIN's to each other will be difficult. It would, unfortunately, be challenging to near impossible to accurately measure or compare a patient match rate – requiring a standard algorithm for all QHINs will make measurements easier to capture and comparison much more possible. There must be checks and balances between the system, the patient, and other medical professionals.

ONC Request for Comment #10: *Recognizing there are different ways to implement Record Location services, should the QTF specify a single standardized approach across QHINs?*

It is important for ONC to establish a common baseline standard across QHINs such that vendors and other entities do not have to complete custom work to meet the inconsistent requirements from QHIN to QHIN. We also encourage the

use of caching, so systems can retain information and systematically know which entity a patient is associated with. This will cut down on the number of broadcast queries over time and make the interoperability ecosystem more efficient.

ONC Request for Comment #11: *Should the QTF require QHINs to implement Directory Services? Recognizing there are many possible approaches for implementing Directory Services, should the QTF specify a single standardized approach? If QHINs implement Directory Services, which entities should be included in directories? Should directories be made publicly accessible?*

Allscripts is supportive of the concepts addressed here and agrees ONC should require QHINs to implement Directory Services. We recommend there be a single standardized approach established that is part of onboarding a Participant, and the directories should absolutely be made publicly available (as noted in comments above). Direct Trust is a good start, though it can be expanded or adjusted over time as merited.

ONC Request for Comment #12: *Future drafts of the QTF will specify a format for Meaningful Choice notices communicated between QHINs. Which standard/format should the QTF specify? What information should be included in a Meaningful Choice notice (e.g., should a notice include patient demographic information to enable QHINs to resolve the identity of the Individual that exercised Meaningful Choice)?*

Allscripts recommends ONC promote a common, consistent standard to ease implementation. We suggest that the end goal should include patients providing approvals or denials via an app on their phone or some other user-friendly mechanism. Meaningful Choice is a highly complex – though worthy – concept, and it is clear that ONC and potentially OCR will need to provide specific details surrounding how to comply with the issue of consent through a range of public educational materials.

ONC Request for Comment #13: *In addition to enabling Meaningful Choice, the Common Agreement requires QHINs to collect other information about an Individual's privacy preferences such as consent, approval, or other documentation when required by Applicable Law. Should the QTF specify a function to support the exchange of such information through the QHIN Exchange Network? Which standards and/or approaches should the QTF specify for this function?*

Allscripts agrees there should be common, consistent standards to manage and exchange individuals' privacy preferences, such as consent, approval or other documentation. We recommend eXtensible Access Control Markup Language (XACML). It can be used for consent and is also applicable across industries.

ONC Request for Comment #14: *QHINs may participate in a variety of activities and transactions involving First Degree Entities and/or internal operations, including receiving and processing Query and Message Delivery Solicitations, performing Patient Identity Resolution, performing Record Location, sending EHI, receiving EHI, performing queries, granting/revoking access credentials, etc. Future versions of the QTF may specify a list of events a QHIN must record involving First Degree Entities and/or internal operations. Which activities and transactions should the QTF specify as auditable events? What information should the QHIN record about each event?*

Allscripts recommends ONC provide a common definition of what would be audited and with whom it should be shared. Right now, that is not entirely clear, and there is room for interpretation in such a way as to cause inconsistency and

even possible accusations of Information Blocking. Providing a clear example of what the audit records should include, in detail, would be helpful too. Ideally, one should be able to tell (from audit reports) where data has been, as well as with whom it has been shared.

ONC Request for Comment #15: *Should the QTF specify a consistent set of error messages for interactions between QHINs? Which error messages should the QTF specify? Should the QTF specify a consistent format for error messages?*

Allscripts agrees the QTF should specify a consistent set of error messages for interactions between QHINs. A predefined catalog of error messages is crucial to driving interoperability forward, and consistently defined data will help.

Allscripts is appreciative of the opportunity to provide feedback to ONC regarding TEFCA. We welcome the opportunity to speak further about any of our feedback or suggestions.

With respect,

Leigh C. Burchell
Vice President, Policy & Government Affairs
Allscripts
(919) 247-1144
leigh.burchell@allscripts.com