The American Medical Association (AMA) appreciates the opportunity to comment on the Office of the National Coordinator for Health Information Technology (ONC) Draft 2 of the Trusted Exchange Framework and Common Agreement (TEFCA). Overall, the AMA supports ONC's goals for the TEFCA, including the ability to (1) provide a single "on-ramp" to nationwide connectivity; (2) enable electronic health information to securely follow the patient when and where it is needed; and (3) support nationwide scalability. We also appreciate ONC rereleasing the draft TEFCA for public comment in conjunction with its information blocking proposals.

Through our direct experience and working with partner organizations, we believe that seamless nationwide sharing of health information is most readily enabled through trust agreements, consistent policy and technical requirements, and appropriate, balanced governance to provide assurance of trust and interoperability. Our experience has proven that an interoperable health information technology ecosystem is best supported through public-private collaboration, grounded in practical implementation that advances interoperable health information sharing and engenders public trust. The AMA supports the congressional intent of the 21st Century Cures (Cures) legislation for greater data liquidity and the potential role of a "trusted exchange framework" as envisioned in that legislation. We appreciate the ways in which ONC has approached development of the TEFCA and its multiple requests for stakeholder input.

That being said, we strongly urge ONC to be mindful of the congressional intent that the TEFCA avoid disruption and duplication of "existing exchanges between participants of health information networks". In our view, as drafted, the TEFCA would both disrupt and duplicate existing exchanges—requiring widespread changes and revisions to the legal terms of thousands of legal agreements. As ONC considers our comments and those of others, we urge it to look for every opportunity to minimize or eliminate such duplication and disruption, especially in the need to revise legal agreements that have, in many cases, taken years to be developed and ratified. For example, we suggest that ONC consider allowing existing agreements to be mapped to minimum required terms and conditions (MRTCs) as a model rather than assuming that current agreements must be revised.

We note the rapid growth of the Carequality trusted exchange framework, which has been specifically designed to reduce variations in participation and data use agreements and includes several implementers who have signed the Carequality Connected Agreement and are in various stages of the onboarding process. The Carequality community includes regional and national health information exchanges (HIEs) and other exchange organizations, including CommonWell and eHealth Exchange. Consistent with congressional intent, the TEFCA should recognize, preserve, and build on this progress.

Furthermore, in reviewing the scope of the TEFCA, and taken in concert with the proposals and request for comment in the recent ONC and Centers for Medicare and Medicaid Services (CMS) Proposed Rules related to interoperability and patient access, the AMA believes the TEFCA necessitates a formal rulemaking process. TEFCA meets the threshold for an economically significant rule given its nationwide scope and anticipated participating entities. Additionally, while ONC has stated that participation in the TEFCA is voluntary, both the ONC and CMS Proposed Rules related to interoperability and patient access sought comment on mandating stakeholder participation (e.g., health information technology vendors and payers). These requests for comment signal the Agencies' intention that all stakeholders participate in the TEFCA, including participation mandated (or de facto mandated) through other government regulations. As such, the TEFCA itself necessitates the formal rulemaking process to ensure appropriate stakeholder participation and federal government impact analysis and review.

Specific Recommendations and Comments

<u>TEFCA language:</u>

> *ONC notes that "[t]he industry has done significant work to broaden the exchange of data, build trust frameworks, and develop participation agreements that enable providers to exchange data across organizational boundaries. A national exchange agreement must leverage what is working well to encourage and facilitate growth."*

The AMA agrees with this observation and underscores the importance of leveraging the substantial number of successful efforts that are underway and minimizing disruption, including the time and resources needed to revise exchange agreements. Fundamentally, the TEFCA should address real, material gaps in current exchange networks, frameworks and agreements. One area where the TEFCA can add real value is in harmonizing agreed upon purposes for exchange.

For example, the development of additional use cases is a major factor in the success of the TEFCA, and therefore, use case development must be a priority for the Recognized Coordinating Entity (RCE). While a broadcast query for treatment purposes is an important aspect of nationwide interoperability, we also foresee the need to replicate high-impact use cases. For instance, many new Alternative Payment Models (APMs) utilize a combination of Certified Electronic Health Record Technology (CEHRT) and custom-developed software to engage patients or manage populations. Results have decreased hospitalizations and emergency room visits, reduced spending, and improved patient satisfaction.[1] **Still, it is extremely difficult for physicians to receive timely and actionable data from payers. ONC should do more to promote the flow of data from the payer to physician.** Replicating these results across the nation will require exposing health IT developers to successful APM health IT frameworks and disseminating the "value proposition" enjoyed by each actor. **To that end, we recommend ONC charge the RCE as a "use case clearinghouse" to help ensure that Qualified Health Information Networks (QHINs), Participants, and Participant Members can accommodate the needs of new care models.**

TEFCA language:

> *ONC will develop the Minimum Required Terms and Conditions (MRTCs), described as "mandatory minimum required terms and conditions with which Qualified Health Information Networks (QHINs) may voluntarily agree to comply." In addition to the MRTCs, the Common Agreement (CA) would include Additional Required Terms and Conditions (ARTCs) that are necessary for an effective data sharing agreement. The RCE will develop the ARTCs and ensure that the ARTCs do not conflict with the MRTCs. ONC will have final approval of the CA.*

The AMA supports the responsibility for the RCE to develop the ARTCs, subject to ONC approval. At the same time, because the ARTCs must be consistent with and not revise the MRTCs, we believe that the RCE should also have an important role in finalizing the MRTCs as well. Both the legal language and operational requirements in the MRTCs would benefit from material RCE input. In addition, it will be important for the RCE to have some discretion to be flexible in application of mandatory CA terms to ensure that the TEFCA can be implemented in as non-disruptive and successful a manner as possible.

TEFCA language:

> *The Trusted Exchange Framework (TEF) Draft 2 refines the concept of a QHIN, which is "an entity with the technical capabilities to connect Participants on a nationwide scale". A QHIN*

[1] Illinois Gastroenterology Group. Proposal to the Physician Focused Payment Model Technical Advisory Committee (PTAC) on Project Sonar. https://aspe.hhs.gov/system/files/pdf/253406/ProjectSonarSonarMD.pdf

> *must meet the definition of a Health Information Network (HIN) and satisfy all conditions of the Common Agreement and accompanying QTF*.

With respect to the definition of a HIN in the TEF Draft 2, the AMA agrees with the definition as bounded QHIN criteria. We expressed concern to ONC that the HIN definition in its recent proposed rule implementing the Cures information blocking provisions is too broad for information blocking enforcement purposes. As a result, we suggest that ONC adopt a unified definition of a HIN for information blocking enforcement and for the TEFCA.

The AMA reiterates its strong recommendation that a definition of HIN (i.e., for both the TEFCA and information blocking regulations) include only entities that are an actual network (or formalized component of an actual network) and have an actual operational role and responsibility for the network. For example, to be a HIN, the network itself provides the ability to locate and transmit electronic health information (EHI) between multiple persons and/or entities electronically, on demand, or pursuant to one or more automated processes. Moreover, to be a HIN, the entity should also be exchanging EHI in a live clinical environment using the network in some capacity.

TEFCA language:

> *The RCE will also be responsible for monitoring QHINs on an ongoing basis and adjudicating noncompliance with the Common Agreement up to and including removal of the QHIN from ONC's public directory on HealthIT.gov, when necessary.*

The AMA recognizes the need, in extreme circumstances, to remove QHINs. ONC should clarify whether the removal of a QHIN would constitute disqualification from participating in the TEFCA. If so, we ask that ONC further clarify how Participant Members would be notified of such an event, how disqualification could impact Participant Members (particularly those participating in the TEFCA via a QHIN as a means to comply with information blocking regulation), and if ONC would consider implementing a corrective action plan prior to disqualifying a QHIN.

TEFCA language:

> *The TEF Draft 2 has a revised set of Exchange Purposes: Treatment, Payment (Utilization Review), Health Care Operations (Quality Assessment and Improvement, and Business Planning and Development), Public Health, Individual Access Service (includes HIPAA right of access and its equivalent), and Benefits Determination.*

The AMA understands the rationale for narrowing Payment and Operations based on comments received and supports efforts where exchange purposes are tailored to certain use cases (e.g., the APM example listed above). We recognize there is a need to expand the number of use cases over time. We note that under the current model, the ARTCs could be not be used in this manner. We suggest that ONC consider enabling the RCE and ARTC process to do so.

TEFCA language:

> *ONC states that QHINs, Participants, and Participant Members must respond to all requests for EHI they receive for any of the Exchange Purposes with the EHI they have available.*

> *As it relates to Participant responses to QHIN Queries, ONC further states that if the Participant stores or maintains EHI, the Participant shall also respond by providing all of the EHI it receives in the then applicable USCDI to the extent that conditions are satisfied.*
>
> *Moreover, when a Participant Member receives a request for EHI from a Participant, ONC states that the Participant Member shall respond by providing all of the EHI in the then applicable USCDI…*

ONC seems to be suggesting that, as a request percolates down to a Participant Member (i.e., a physician's practice), the physician is ultimately responsible to provide the USCDI, and such information would constitute EHI for purposes of meeting the Participant Member minimum obligations under the TEFCA. It is unclear, but we assume that ONC is establishing nested requirements (i.e., QHIN to QHIN, QHIN to Participant, Participant to a Participant and so on), meaning that a physician is responsible only for EHI that can be provided using CEHRT—in other words the USCDI. If this is the case, the AMA appreciates ONC's practical approach for creating a "common denominator" of structured, computable information in the TEFCA. **We support exchanging and accessing information that is useful and accommodates the needs of those who require information for a particular purpose.**

However, an alternative read would be to say TEFCA requires the access, use, and exchange of all EHI where only a subset is formatted to comply with the USCDI, while all other EHI must be shared in whatever means a QHIN, Participant, or Participant Member chooses. **This approach would run contrary to what physicians have been demanding for years and would not constitute meaningful interoperability.** Not only would this increase the variability of information shared via the TEFCA—devaluing the "trust" and "common" aspects of the TEFCA—but also would significantly increase the volume of data a physician or patient must manually "dig through" in hopes of finding pertinent information.

The AMA has expressed serious concerns to ONC that the definition of EHI is too broad. Our Cures regulatory comments provide several examples where ONC's information blocking proposals and definition of EHI will negatively impact patient privacy, data security, health system efficiency, and physician burden. ONC's interpretation of Cures' terms "information blocking" and "EHI" places major expectations on the actors involved. The AMA reiterates caution and to consider downstream consequences of being too broad or expansive. We are very concerned that ONC's EHI and information blocking proposals are too vague, using many undefined terms (e.g., timely, burdensome, network, etc.). This vagueness creates uncertainty around whether information blocking can be objectively evaluated and validated by HHS, potentially weakening this important Cures provision. A logical, objective approach to promoting interoperability is necessary to reduce confusion. **This is just as necessary in developing the TEFCA.** The USCDI provides structure, using standards that move us closer to a computable medical record. As such, **ONC should align its information blocking and TEFCA requirements with its own certification requirements. In other words, EHI requirements in TEFCA should be evaluated through the lens of access, use, and exchange of the USCDI.**

We are also concerned about the sustainability of the TEFCA model, including the fees associated with participating in or making queries via the QHINs and the viability of QHINs over time. TEFCA appears to not require public fee reporting and only requiring a QHIN to "file with the RCE a schedule of Fees used by the QHIN relating to the use of the QHIN's services provided pursuant to the Common Agreement that are charged to other QHINs and Participants." It is unclear whether the RCE would then make this information public to Participants and Participant Members.

We urge ONC to clarify that fees charged by a QHIN must be made publicly available, whether by the QHIN itself or via the RCE. ONC should ensure that QHINs using a transaction fee or similar model are required to provide the associated fee after the Participant inputs the query and before the QHIN completes the query. This will ensure physicians are not hit with surprise fees. Lastly, the AMA is concerned that a diminishing number of QHINs over time could lead to higher prices for Participants and Participant Members. This is especially problematic if physicians find that belonging to a QHIN advances better patient care, yet participation is not feasible, or, alternatively, physicians feel they may risk regulatory consequences for lack of participation. To address these concerns, ONC and the RCE should ensure reasonable and consistent fees across QHINs **and reassure physicians that participation under the TEFCA is not a requirement (and will not become a de facto requirement) and that there be a safe harbor from penalties associated with information blocking.**

TEFCA language:

> *ONC indicates that it intends to "phase in new exchange modalities and Exchange Purposes in the Common Agreement to support additional use cases". ONC also states that, as it phases in new requirements, "QHINs, Participants, and Participant Members are in no way limited from voluntarily offering additional exchange modalities and services or from entering into point-to-point or one-off agreements between organizations that are different from the Common Agreement's MRTCs, provided that such agreements do not conflict with the policies of the Common Agreement". It emphasizes that the "TEF and the Common Agreement do not limit the ability of HINs to innovate and build additional services that would provide value to their users and support their long-term sustainability".*
>
> *ONC intends to work with the National Institute of Standards and Technology (NIST) and the industry on pilots focusing on use cases of the TEF and the Common Agreement.*

The AMA notes that ONC has not sufficiently addressed an important component of Cures as it relates to the TEFCA. Cures requires ONC to work with the National Institute for Standards and Technology (NIST) around interoperability pilot tests:

> ''(iii) PILOT TESTING.—The National Coordinator, in consultation with the National Institute of Standards and Technology, shall provide for the pilot testing of the trusted exchange framework and common agreement established or supported under this subsection (as authorized under section 13201 of the Health Information Technology for Economic and Clinical Health Act). The National Coordinator, in consultation with the National Institute of Standards and Technology, may delegate pilot testing activities under this clause to independent entities with appropriate expertise."

We agree use case pilot testing is an important component in establishing a functional TEFCA, however, limiting the testing to just use cases misses congressional intent. We believe Congress included the above provision to ensure potential issues with the TEFCA are ironed out before it goes live. For instance, given the complexities, interdependencies, costs, and potential burdens of establishing, managing, and deploying a nationwide identity proofing process, **the AMA strongly urges ONC to pilot test, in consultation with NIST, any and all identity proofing methods considered for use in a national trusted exchange framework prior to finalizing the TEFCA.** Considering the importance of managing access, authorization, and authentication at this scale, ONC would be remiss to not leverage appropriate pilot testing to bolster confidence and trust in the privacy and security of patient health information.

Additionally, the AMA recommends a phased approach to TEFCA implementation with clearly delineated milestones and pilot testing, as mandated by the statute. The likelihood of success would

improve by phasing in the supported purposes and use cases over time. The permitted purposes outlined in the TEFCA will require considerable time and resources to implement and may initially be out of reach for some HINs and Participants. **Specifically, the AMA recommends that the first phase focus on the exchange of information for treatment and patient access to information, with a corresponding pilot test in certain geographic areas.** This should be followed by a second phase focused on expanding these sharing and patient access functions nationally. Subsequent phases could focus on implementing the sharing of information for health care operations and payment purposes.

We also urge ONC to clarify that providing a patient with access to EHI that is not directly maintained by the Participant or Participant Member is the responsibility of the QHIN. To do otherwise places an extraordinary burden—of both time and potentially associated fees—on physicians to query and provide access to multiple records that do not exist in their systems. In providing this clarification, **ONC should permit physicians to direct patients to the QHIN for access to their EHI and ensure HINs are appropriately situated to respond to and fulfill these patient inquiries as a condition of becoming a QHIN.**

TEFCA language:

> *Participants and Participant Members must comply with the HIPAA Privacy and Security Rules and Applicable Law, when applicable. However, regardless of whether they are a Covered Entity or Business Associate, Participants and Participant Members must take reasonable steps to promote the confidentiality, integrity, and availability of EHI, including maintaining reasonable and appropriate administrative, technical, and physical safeguards for protecting EHI; protecting against reasonably anticipated impermissible Uses and Disclosures of EHI; identifying and protecting against reasonably anticipated threats to the security or integrity of EHI; and monitoring workforce compliance. ONC is requesting public comment regarding appropriate security controls for Participants or Participant Members in the Common Agreement, specifically regarding EHI received from federal agencies.*

The AMA appreciates the flexibility of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule's requirements because physician practices are varied and have different security needs, resources, and skill levels. Many practices understand that they need robust plans to ensure their systems and patients are protected yet struggle with conducting security risk analyses as outlined by HIPAA. Thus, ONC should permit "multiple paths to compliance". Participant Members that adopt and implement a security framework (such as the NIST Cybersecurity Framework) or take steps toward applying the Health Industry Cybersecurity Practices[2] (the primary publication of the Cybersecurity Act of 2015, Section 405(d) Task Group) should be considered as appropriately meeting security controls. This is an important step in helping make cybersecurity more understandable and attainable to physicians, particularly those that are most vulnerable due to lack of resources and expertise. The whole health care

[2] HHS Office of the Assistant Secretary for Preparedness and Response, Health Industry Cybersecurity Practices, (2018). By way of background, in 2015, Congress passed the Cybersecurity Act of 2015 (CSA), which includes Section 405(d), Aligning Health Care Industry Security Approaches. In 2017, HHS convened the CSA 405(d) Task Group, leveraging the Healthcare and Public Health (HPH) Sector Critical Infrastructure Security and Resilience Public-Private Partnership. The Task Group is comprised of a diverse set of over 100 members representing many areas and roles, including cybersecurity, privacy, healthcare practitioners, Health IT organizations, and other subject matter experts. The Health Industry Cybersecurity Practices they developed aim to raise awareness, provide vetted cybersecurity practices, and move organizations towards consistency in mitigating the current most pertinent cybersecurity threats to the sector. The publication seeks to aid healthcare and public health organizations to develop meaningful cybersecurity objectives and outcomes.

system—including patients—benefits when protected health information is kept private and secure. The NIST Cybersecurity Framework and the Health Industry Cybersecurity Practices best practices utilize industry experts to identify the most pressing risks and develop safeguards to help to address these risks.

TEFCA language:

> *ONC states that "[e]Establishing baseline privacy and security requirements shared by all QHINs, Participants, and Participant Members is important for building and maintaining confidence and trust that EHI shared pursuant to the Common Agreement is appropriately protected".*
>
> *"[…] the Common Agreement requires non-HIPAA entities, who elect to participate in exchange, to be bound by certain provisions that align with safeguards of the HIPAA Rules. This will bolster data integrity, confidentiality, and security, which is necessary given the evolving cybersecurity threat landscape."*
>
> *The MRTCs Draft 2 requires that QHINs, Participants, and Participant Members enable individuals to exercise Meaningful Choice to request that their EHI not be used or disclosed via the Common Agreement, except as required by law.*
>
> *ONC is considering inclusion of a new security labeling requirement. Recognizing that Data Segmentation for Privacy (DS4P) and the associated HL7 implementation guide have not received wide adoption, ONC indicates that it is considering a somewhat focused security labeling policy.*

The AMA strongly agrees with the need to ensure patient data is private and secure. The first step of any ultimately successful privacy framework places the patient first. Each entity seeking access to patients' most confidential medical information must pass the stringent test of showing why its professed need should override individuals' most basic right in keeping their own information private—something that technology should help physicians accomplish in a minimally burdensome way. Moreover, citizens deserve a full and open discussion of exactly who wants their private medical information and for what purpose.

We support requiring QHINs, Participants, and Participant Members to comply with the HIPAA Breach notification requirements "regardless of whether or not they are a Covered Entity or Business Associate," as well as requiring QHINs to "notify the RCE, as well as other QHINs, Participants, Participant Members, and Individual Users who may have been affected by the Breach without unreasonable delay."

We support that "meaningful choice" would be prospective only, as a retrospective requirement would be unduly burdensome and impracticable. We request clarification regarding how the "meaningful choice" requirements under the TEFCA interact with state information sharing requirements, which can vary from "opt-in" (e.g., the individual must give affirmative consent to share information) to "opt-out" (e.g., the information is shared unless the individual opts-out).

We appreciate ONC's attention on data labeling, consent, and requirements on non-HIPAA entities. The AMA has heard concerns from consumer groups and patient advocates about the volume, variety, and velocity of data shared without assurances of privacy and security. Segmenting and identifying sensitive data are crucial in protecting patient privacy. Yet, standards for data labeling are not currently mature enough to implement in the near-term. The AMA instead recommends including security labeling over time as standards mature and as the infrastructure to support it grows.

We appreciate that ONC is proposing Consent2Share (C2S) and DS4P as certification criteria in its 2015 Edition CEHRT update. With regards to security labeling, it is unclear how TEFCA participants will achieve the goal of protecting sensitive data if there is not widespread availability of technology that supports segmentation and consent. TEFCA also states that the Participant or Participant member will obtain and maintain copies of that consent and make it available to other Participants and QHINs as needed. Physicians currently routinely obtain consent from individuals in the course of providing services, but it is unclear what mechanism would be available to allow physicians to electronically track consent (and changes in consent) and enable this information to move swiftly and efficiently from the Participant (or Participant Member) to the QHIN.

ONC's labeling and consent management proposals adds weight to the AMA's **recommendation to require C2S in Base EHR certification as part of ONC's proposed changes to 2015 Edition CEHRT.** This will help develop the foundation for a national privacy framework. In discussions with the Substance Abuse and Mental Health Services Administration (SAMHSA), we have learned that Fast Healthcare Interoperable Resources (FHIR)-enabled C2S provides for both physician and patient-facing services and the infrastructure to segment data and manage consent. **Additionally, we strongly encourage ONC to promote C2S maturity and adoption.** We are aware that there is no longer funding to continue this important work. **The AMA recommends ONC coordinate with SAMHSA to establish a public-private project to advance C2S.** ONC should consider modeling this process off of the Da Vinci Project. Vendors and payers have expressed the need to address "the dual challenges of data standardization and easy information access" with the goal "to help payers and providers to positively impact clinical, quality, cost and care management outcomes."[3] As such, we expect health IT vendors and payers would welcome a public-private C2S effort. **We also recommend ONC direct the RCE to support C2S maturity.**

The AMA has also identified an opportunity for multiple coexisting components to empower patients with meaningful knowledge and control over the use of their data. If patients access their health data—some of which could contain family history and could be sensitive—through a smartphone, they must have a clear understanding of the potential uses of that data by application (app) developers. Most patients will not be aware of who has access to their medical information, how and why they received it, and how it is being used (for example, an app may collect or use information for its own purposes, such as an insurer using health information to limit/exclude coverage for certain services, or may sell information to clients such as to an employer or a landlord). The downstream consequences of data being used in this way may ultimately erode a patient's privacy and willingness to disclose information to his or her physician.

ONC itself highlights these concerns in TEFCA:

> Individuals, health care providers, health plans, and networks may not be willing to exchange data through the Common Agreement if smartphone app developers and other non-HIPAA entities present privacy or security risks because they are not obligated to abide by the HIPAA Rules. In order to meet the goals of the Cures Act as well as to help address these concerns and encourage robust data exchange that will ultimately improve the health of patients, the Common Agreement requires non-HIPAA entities, who elect to participate in exchange, to be bound by certain provisions that align with safeguards of the HIPAA Rules.

[3] Health Level 7, Da Vinci Project, available at: http://www.hl7.org/about/davinci/.

We believe that ONC has the responsibility to provide patients with a basic level of privacy and app transparency—especially since some apps deliberately hide their actions and make it difficult for patients to learn about or control their data.[4] The AMA urges ONC to take the following steps to ensure patient data are accessed, exchanged, and used pursuant with the goals outlined in Cures and the desires expressed by patients.

As part of the Participant Minimum Obligations, those Participants who are also API Technology Suppliers **should require their APIs check an app's attestation to:**

- **Industry-recognized development guidance;**
- **Transparency statements and best practices; and**
- **The adoption of a model notice to patients.**

One possible method to accommodate this would require a Participant's (e.g., EHR vendor) API to check for three "yes/no" attestations from any consumer-facing app. For example, 1) An app developer could choose to assert conformance to Xcertia's Privacy Guidelines.[5] 2) An app developer could attest to the Federal Trade Commission's (FTC) Mobile Health App Developers: FTC Best Practices and the CARIN Alliance Code of Conduct. 3) An app developer could attest to adopting and implementing ONC's Model Privacy Notice. We would urge Participants—and potentially the RCE—to publicize the app developers' attestations.

Permitted and Future Uses of EHI

The MRTCs lay out the permitted and future uses of EHI for QHINs (§ 2.2.2), Participants (§ 7.2), and Participant Members (§ 8.2). While the AMA generally agrees with the uses, we seek clarification as to why QHINs can use the EHI for broader purposes. Specifically, both Participants and Participant Members must be a Covered Entity or Business Associate to be allowed to use data as otherwise permitted by Applicable Law. However, QHINs have no such Covered Entity or Business Associate requirement. Accordingly, the AMA asks that QHINs be held to the same requirements as Participants and Participant Members for permitted and future uses so that "otherwise permitted by Applicable Law" is restricted to QHINs that are Covered Entities or Business Associates.

Government as a Participant or Participant Member

The MRTCs allows for federal agencies to serve as a participant (§ 7.21) or a participant member (§ 8.21) and are not otherwise subject to the HIPAA Rules if they are not already required to comply with the HIPAA Privacy and Security Rules. Although these federal agencies will still need to comply with all other privacy and security requirements imposed by applicable federal law, the AMA has serious concerns allowing the government access to an individual's EHI for Exchange Purposes.

First, the AMA seeks clarification about the interaction of the definition of Exchange Purposes and sections 7.21 and 8.21. The definition of Exchange Purpose states that EHI may be requested under 2.2.1, 7.1, and 8.1 only for an Exchange Purpose of a Covered Entity or other health care provider that is acting

---

[4] Kit Huckvale et al., JAMA Netw Open. 2019;2(4):e192542, *Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation* (April 19, 2019), available at https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2730782?utm_source=For_The_Media&utm_medium=referral&utm_campaign=ftm_links&utm_term=041919.

[5] Both the Food and Drug Administration (FDA) and ONC participate on the board of Xcertia, a multi-stakeholder effort to develop guidelines and recommendations for medical app development.

in accordance with Applicable Law. Does a federal agency's request under either 7.21 or 8.21 fall with the restriction set out in the definition of Exchange Purpose?

Second, even if a federal agency's request falls within the definition of Exchange Purposes, the AMA has serious concerns because benefits determinations are explicitly excluded from the above Exchange Purpose definition. Thus, federal agencies could use the information available through the TEF to determine eligibility for federal government programs without individual's knowledge or consent. Such use of information does not protect public health or encourage access to needed medical care.

Comments on Participant Member Minimum Obligations

As an overarching concern, **the AMA urges ONC to maintain the voluntary nature of the TEFCA, specifically that physicians cannot be deemed "information blockers" if they determine that participation under the TEFCA is not optimally serving their patients or that such participation is not possible due to EHR limitations or burden, including associated costs.** Mandatory or de facto mandatory participation requirements imposed by EHR vendors, payers, or the federal government would place physicians at a distinct disadvantage relative to QHINs should physicians determine, for example, that there are deficiencies with the QHIN network, including information security or fees for membership or queries.

For "8.8 Authorization," we ask ONC to confirm whether this provision applies to QHIN-to-Participant Member transactions, which should be provided proactively by the QHIN and addressed by the QTFs, or does it also apply to Participant Members querying through the QHIN. Greater clarity would be helpful.

For "8.9 Identity Proofing," and "8.10 User Authentication," we are concerned that rigid and universal required operational application of these requirements for QHINs, Participants, and Participant Members could deter organizations from participating in the TEFCA. It is not clear if ONC intends for each QHIN to provide identify proofing services for its Participants and Participant Members, i.e., top down, or if QHINs will provide a one identity proofing service while Participants provide yet another, i.e., distributed and non-centralized. The AMA supports the ultimate goal of reducing the friction and cost associated with identify proofing. However, given the confusion around ONC's approach, the AMA requests further clarity. For instance, if a QHIN provides an identify proofing service for all of its Participants and Participant Members how would this service be managed, distributed, and funded? Would all physician offices be required to implement new software and services for identify proofing patients? Furthermore, what educational process will be developed to ensure all individuals are clear on the use and security of the identities?

For "8.16 Data Integrity," we question the value of the statement that "[e]ach Participant Member shall report known instances of inaccurate or incomplete EHI to the originator of the EHI, and request that such data integrity issues be remediated in a timely manner to the extent reasonably possible." This provision does not distinguish between a QHIN, Participants, Participant Members, or those of another QHIN. More fundamentally, when would a Participant Member know if EHI is inaccurate and how is "incomplete" defined? It is unclear when a Participant Member would have the data access or information to identify such issues.