ciitizen

June 17, 2019

Dr. Don Rucker, MD
National Coordinator for Health Information Technology
Office of the National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

RE: 21st Century Cures Act Trusted Exchange Framework and Common Agreement (v2) Comments

Dear Dr. Rucker:

Ciitizen's mission is to empower the world's seven billion citizens to have complete control of their health data: to share it with whomever, whenever, and wherever they want. With a focus on empowering sick patients, beginning with cancer, the Ciitizen online platform democratizes health care by putting data ownership and control back in the hands of patients – the stakeholders most highly motivated to collect it, use it, and share it liberally to save their own lives and the lives of others just like them.

Ciitizen leverages the HIPAA Privacy Rule's individual right of access, as well as capabilities in certified electronic health record technology (CEHRT), in order to populate a user's Ciitizen profile. Our cancer patient users, with their complete, relevant health histories in hand, will be empowered to seek treatment options, help their providers better coordinate their care, and contribute their data to research and other population health initiatives, such as value-based care programs.

We believe in the enormous potential for the Trusted Exchange Framework (and the ecosystem it empowers – referred to herein as the "TEF") to enable individuals, on their own and through applications and services working on their behalf, to more easily access their health information from wherever it resides, through a single on-ramp. We support most aspects of version 2 of the Trusted Exchange Framework and Common Agreement (TEFCA), including the inclusion of "push" messages, as well as query/response methods of exchange. In our comments to the first draft of the TEFCA, we expressed concerns about how individuals and their chosen apps would be able to leverage the framework, including whether consumer-facing apps would be required to make information available for all of the permitted purposes in exchange for the opportunity to obtain their health information. We appreciate ONC's efforts to resolve those concerns in this second draft of the TEFCA. However, we continue to have questions about how TEF will be operationalized for individuals and their chosen apps and have a number of suggestions we believe will improve the ability of the TEF ecosystem to facilitate compliance with an individual's HIPAA Right of Access.

In summary:

- ONC (and the RCE) should assure that there are opportunities for apps serving the needs of individuals to have a viable on-ramp to the TEFCA ecosystem.

- ONC should assure that any privacy and security requirements established for consumer-facing apps that are Participant Members do not create barriers to the exercise by an individual of their HIPAA Right of Access through the app of his or her choice.
- We support the prohibition on fees charged by one QHIN to another for exchange to support Individual Access Services but note that any fees imposed on individuals (or apps acting on their behalf) for Individual Access Services should be in compliance with the HIPAA Right of Access, as well as any applicable fee restrictions in the Information Blocking Rules.
- The TEFCA should support access to all EHI that is part of the designated record set and that is available via any QHIN regardless of whether the data requested is or is not in the USCDI.
- ONC should ask OCR to issue guidance or proposed rules clarifying the right of business associates under the 21st Century Cures Act to directly comply with an individual's HIPAA Right of Access request notwithstanding contrary or unclear provisions in their business associate agreements.
- Once an individual's app has received EHI via the TEF, any further uses or and disclosures of that information should be up to individual and not subject to restrictions imposed by terms of the Common Agreement or additional requirements imposed by the RCE, QHINs, Participants, or Participant Members.
- We strongly support provisions that prohibit requiring a HIPAA authorization or a business associate agreement to provide Individual Access Services.
- Breaches should only be required to be reported to individuals, to applicable federal (and/or state) authorities (those that can hold the entity accountable), and to only those Participant Members, Participants, or QHINs directly affected by the breach (i.e., the breach suggests a security issue for that entity or triggers a potential notification requirement).
- Notwithstanding OCR prior guidance on this issue, ONC should not permit QHINs, Participants, and Participant Members to insist on their own forms for Individual Access Services.
- We urge ONC to clarify how consumer-facing apps will be able to comply with the proposed IAL2 requirements.
- Individuals should be permitted to opt-out (exercise Meaningful Choice) of participating in the TEF for other Permitted Purposes but still be permitted to request Individual Access Services (either individually or through the app of their choice).
- The required information in the summary of disclosures in Section 9.5.2 should not require information that is not already automatically collected by the technology as part of the workflow of requesting or disclosing the EHI.
- Information received by a QHIN, Participant, or Participant Member in order to fulfill Individual Access Services should be passed on to its destination (the individual or the individual's app) and not retained or held by the conduit for any longer than is necessary to assure the access request has been honored.
- We support how the draft TEFCA handles the federal and state law consent requirements, placing the obligation on the entity subject to the consent law to obtain the consent prior to releasing information – but question whether there is any additional value to the proposed privacy labeling (such as through DS4P).
- Exceptions to nondiscrimination provisions should not be interpreted to prohibit individuals from requesting Individual Access Services via the TEF through the app of their choice.

Assuring Individuals and Consumer-Facing Apps can Access the TEF for Individual Access Services

We read the revised draft TEFCA as requiring consumer-facing apps to become a Participant Member (PM) in order to leverage the TEF for Individual Access Services. Although we appreciate that ONC has responded to our prior concerns regarding a lack of clarify regarding how consumer-facing apps could leverage the TEF, we have concerns that some of the proposed Minimum Required Terms and Conditions

(MRTCs) on PMs, as well as the prospect of Additional Required Terms and Conditions (ARTCs) which would be imposed by the RCE (or by individual QHINs or Participants), could create obstacles to consumer-facing app participation or the viability of the TEF to support compliance with the HIPAA individual Right of Access.

In order for Ciitizen as a PM to leverage the TEF, it appears the MRTCs will require us to become a member of at least one Participant or QHIN (e.g., HIE). Because HINs are free to impose their own requirements (including fees), as long as they are not in violation of the Common Agreement or other applicable law, it's not clear whether there is a viable pathway for consumer-facing apps. Today there are few if any HIEs that have consumer-facing apps as members - in fact, today few if any HIEs are responding to requests by individuals or their apps pursuant to the HIPAA Right of Access, likely due to business associate agreement constraints or a lack of prioritization of this use case. If ONC continues to see individual apps as Participant Members (vs. expanding the definition of "individual" to include apps working on an individual's behalf), it will be critical to assure there is at least one QHIN or Participant that can serve as the on-ramp for individual requests, whether they come directly from an individual or from an app working on the individual's behalf. (The other potential option is for a consumer-facing app to rely on another Participant Member (PM), such as a health care provider or health plan – but concerns remain about possible conditions that could be imposed by such a PM.)

We applaud and support provisions in the MRTCs that make clear that HINs cannot require a consumer-facing app to execute a business associate agreement or complete a HIPAA authorization in order to facilitate Individual Access Services[1] (but see footnote for on an exception to this with respect to caregivers). **We also applaud and support the MRTC provision making clear that consumer-facing apps (PMs) who are participating in the TEF solely for the purpose of facilitating Individual Access Services are not required to release EHI for any of the other Permitted Purposes.** However, we note consumer-facing apps should be able to, at the request of an individual, share data back for any of the Permitted Purposes via the TEF without necessarily having to agree to have their data open for queries for all of the Permitted Purposes. In other words, individuals will need their apps to be able to use a single on-ramp to both query for their EHI and also share data back (such as with medical providers for treatment) on a case by case basis.

<u>Assuring the TEF can Facilitate Compliance with the HIPAA Right of Individual Access</u>

Ciitizen appreciates the privacy and security requirements imposed on Participant Members, including those that are consumer-facing apps, and – subject to a few comments below regarding restrictions on subsequent uses and disclosures of EHI, requirements to meet IAL2 for identity proofing, breach notification, and summary of disclosures – we could meet those requirements. However, imposing these requirements could limit the ability of individuals to leverage the TEF to obtain their health information pursuant to the HIPAA individual Right of Access. OCR recently released guidance[2] to further clarify that

[1] The HIPAA Right of Access can be exercised only by the individual and personal representatives, who are individuals with the legal authority to make decisions about a person or executors/heirs to the estate of a deceased person. The definition of "individual" in the TEFCA includes individuals who are acting on behalf of another (such as a caregiver without legal representative status). Such individuals are not permitted to exercise the right of access; consequently, a request for EHI from such an individual would either need to be accompanied by a HIPAA authorization or may be able to be accomplished by a HIPAA covered entity (or business associate acting on its behalf) pursuant the provisions permitting (but not requiring) sharing with friends and family of information relevant to their assistance in helping to care, or pay for care, for that individual. Note that once an individual has obtained their health information, they are free to authorize caregivers (and de-authorize, in accordance with their preferences) to access that information.

[2] https://www.hhs.gov/hipaa/for-professionals/faq/health-information-technology/index.html#access-right,-apps-

individuals have the right to have protected health information in a designated record set sent to the third party of their choice, and that concerns about the privacy and security practices of those third parties cannot be used as an excuse not to exchange data.

For example, Sections 5.1.2, 7.5, and 8.5 of the TEFCA permit HINS (QHINs, Participants, and Participant Members) to discriminate in TEF-related services "based on a reasonable and good faith belief that the entity or group has not satisfied or will not be able to satisfy the applicable terms of the CA (including compliance with Applicable Law) in any material respect." In addition, the TEF principles state that HINs "should not limit third party applications from accessing individuals' EHI via an API *when the application complies with the applicable data sharing agreement requirements,*" which makes clear that only those apps that agree to sign data sharing agreements (for which the terms are unknown) could be utilized by individuals to request Information Access Services.

We have concerns about these provisions, because they put entities with health information that individuals have a right to access (and their business associates) in a position to decline to honor an individual's access request on the basis that the recipient (such as app) selected by the individual has unreasonable or insufficient (in the views of the entity) privacy and security practices. HIPAA, as amended by HITECH, gave individuals the choice to have their health information sent to the third party (person or entity) of their choice, without the caveat that this third party be compliant with HIPAA or any other minimum privacy and security practices. It is already the case that neither a HIPAA covered entity nor a business associate is legally responsible for privacy and security practices of downstream recipients of PHI, as long as the disclosure of the information to that recipient is HIPAA-compliant. In the case of an individual sending information to an app or another third party, this provision puts entities in the position of judging the privacy and security posture of recipients, even though the law does not hold data providers responsible for downstream uses of the information. We question the purpose for this provision and urge that it be modified to more specifically address the concern it was intended to address (vs. leaving this as a judgement call for a QHIN, P or PM).

Except as noted in these comments, we believe we could meet the MRTCs – but we have concerns about additional requirements that might be imposed as ARTCs or be imposed by individual QHINs, Participants, or Participant Members who are the "gateway" to TEF access. **We urge ONC to impose additional constraints on the ability of TEF stakeholders to impose additional requirements on consumer-facing apps in ways that would frustrate the ability of the TEF to serve as a viable ecosystem for exercise of the individual's HIPAA Right of Access.**

Of particular concern are additional fees for participation. The draft MRTCs preclude the imposition of fees among QHINs for facilitating Individual Access Services but say nothing about fees imposed by Participants or Participant Members. At a minimum any such fees for Individual Access Services must be compliant with the HIPAA Right of Access and, as applicable, the Information Blocking rules.

The MRTCs require stakeholders participating in the TEF to respond to queries only with data that is part of the then-current USCDI. Because the USCDI falls short of the HIPAA Privacy Rule designated record set (and will for some years to come), this limits the ability of the TEF to be leveraged for compliance with the HIPAA Right of Access. **Sharing of EHI through the TEF is not dependent on the use of FHIR APIs, therefore the limitation to the USCDI makes less sense. We urge ONC to modify the MRTCs to require QHINs, Participants, and Participant Members to make any EHI in that they possess or are able to access available at least for Individual Access Services (and at least to the extent the EHI meets the definition of**

---

and-apis

the designated record set in HIPAA). For example, we could see imaging services robustly participating in the TEF to make images available for the Permitted Purposes – but images are not likely to be part of the USCDI until future versions. As we have noted in our recent comments to ONC's proposed interoperability and information blocking rules, the ability for individuals (or apps working on their behalf) to exercise their Right of Access is much harder than it should be today, and we urge ONC to use all of its authorities – including the TEFCA – to facilitate the HIPAA Right of Access to the maximum extent possible.

Finally, we note again that many of the stakeholders that ONC hopes will participate in the TEF, and particularly the QHINs and Participants, will be business associates under HIPAA. As noted above, few HIEs today are directly responding to requests from individuals (or apps working on their behalf) seeking to exercise their HIPAA Right of Access. Congress in the 21st Century Cures Act paved the way for business associates to voluntarily provide individuals with the right to access their health information, at least with respect to information that comes from an "electronic health record" (which is defined in HITECH broadly and not just limited to certified EHR technology).[3] Section 4006(b) of the 21st Century Cures Act (P.L. 114-255), which amended HITECH, provides as follows:

> if the individual makes a request to a business associate for access to, or a copy of, protected health information about the individual, or if an individual makes a request to a business associate to grant such access to, or transmit such copy directly to, a person or entity designated by the individual, a business associate may provide the individual with such access or copy, which may be in an electronic form, or grant or transmit such access or copy to such person or entity designated by the individual….

However, it is not clear that many BAs have done so given the absence of implementing regulations in the HIPAA Privacy Rule. The Cures statutory provision provides BAs with sufficient legal authority to act, at least with respect to PHI that comes from an "electronic health record" as that term is defined in HITECH – but where the BAA has contrary or less than clear language, BAs will be reluctant to take on potential liability in making information directly available to individuals. We have spoken with a number of BAs (health information exchanges in particular) who are interested in enabling individuals to have direct access to their PHI but are hesitant due to lack of clarity from OCR and/or contrary or unclear provisions in their BAAs. This will impact the ability of business associates to participate in the TEF and fulfill Individual Access Services.

ONC should ask OCR to promptly issue guidance to at least enable BAs who seek to rely on the Cures language in Section 4006(b) to provide individuals directly with access to be able to do so, regardless of existing provisions in the BAA, and provide them (and the covered entities with whom they contract) a generous grace period for revising BAAs to make them consistent with both 21st Century Cures and the decision of the BA to opt into providing individual access. OCR did this with respect to implementation in BAAs of the HITECH changes in the Omnibus regulations.[4] For those BAs who make PHI directly available to individuals seeking to exercise their right of access, OCR should fully enforce 45 CFR 164.524 against entities who fail to provide such access in accordance with the Privacy Rule.[5] Otherwise, covered entities

[3] Section 13400(5) of HITECH defines and "electronic medical record" as an "electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff."

[4] See discussion of transition provisions at 78 Fed. Reg. 5566, at 5602-03 (January 25, 2013).

[5] Potentially relevant statutory authorities: Section 4006(b) of the 21st Century Cures Act (P.L. 114-255) expressly amended the HITECH Act to make clear that if an individual makes a request to a BA under the individual right of access, the BA may provide that individual (or his or her designee) with the requested access or copy. Section 13404 of the HITECH Act provides that the "additional requirements of this subtitle that relate to privacy and that are made applicable with respect to covered entities shall also be applicable to such a business associate…".

would have liability for BA noncompliance – which further complicates the willingness of BAs to participate in the TEF.

Other Potential Obstacles to Consumer-Facing App Participation in the TEFCA

We note that Sections 7.1(ii) and 8.1(ii) of the MRTCs further limits the ability of Participants and Participant Members who are participating in the TEF to facilitate Individual Access Services from using or disclosing any EHI received via the TEF for any reason but to facilitate Individual Access Services.[6] **There are significant challenges for all potential TEF stakeholders regarding separately maintaining EHI based on its source** (of note, HIPAA treats all PHI (with the exception of psychotherapy notes) equally, regardless of its source). But for consumer-facing apps who are leveraging the TEF primarily for Individual Access Services, this constraint impairs the ability of consumers to then be able to access, use and share that EHI for any purpose he or she chooses, consistent with the idea that personal health records are designed to be consumer-controlled. We note also that this is in conflict with MRTC 9.2, which provides individuals with the right to use and disclose their EHI without limitations. Further, an individual might want his or her app to be able to leverage the TEF not just to acquire data through Individual Access Services but to also be able to share that data back for one or more of the other Permitted Purposes as they choose– but without having to agree, as a condition of receiving EHI, to open their accounts for all of the Permitted Purposes, for all requesters. **ONC should modify the TEFCA to enable consumer-facing apps who participate in the TEF to be able to serve the interests of their users in having complete health care records under their complete control (without restrictions that are arguably designed more for a provider, health plan, or HIE).**

We note the following in case ONC decides to allow consumer-facing apps participating in the TEF to further use and disclose EHI sourced via the TEF if permitted by the individual pursuant to an authorization that meets the "Minimum Information" definition. We greatly appreciate ONC's efforts to define the elements of Minimum Information in a way that, in theory, facilitates more informed consent. However, it will be overwhelming for consumers to receive all of this information about each and every disclosure, and more likely result in consumers failing to read any of the provisions[7] and skipping to the bottom to consent. Informed consent with respect to data uses and disclosures is truly a challenge, as we desire to be fully transparent with individuals about what is happening with their data – and yet a longer consent or notice will rarely be read. Many of the components of the Minimum Information definition are frequently covered as part of an app's terms of service or privacy policy – and while it is the case that few consumers read these documents, that problem does not get fixed by jamming all of that information into each and every use or disclosure request. **ONC's proposal to require completion of the Model Privacy Notice is likely the most effective way to get consumers with valuable information on how an app will access, use, and disclose their personal information – and the consent form itself can be more limited to the essential aspects,** such as who is being provided with access to the data, and where possible, for what purpose and for how long.

[6] Overall, the TEFCA – while contemplating that personal health record vendors would be PMs – tends to treat HINs as though they are all either providers or HIEs. For example, the TEF Principles state that "HINs should clearly specify the minimum set of uses and disclosures for exchanging EHI and, for non-treatment purposes, limit the use of EHI to the minimum amount required." This provision makes little sense for a consumer-facing app that is a PM, where access, use and disclosure of EHI should be under the control of the consumer.

[7] For further discussion of the paradox of consent, see, for example, https://www.cdt.org/files/healthprivacy/20090126Consent.pdf; Barocas, S., Nissenbaum, H.: Big data's end run around anonymity and consent. In: Lane, J., Stodden, V., Bender, S., Nissenbaum, H. (eds.) Privacy, Big Data, and the Public Good: Frameworks for Engagement, pp. 44–75. Cambridge University Press, Cambridge (2014).

The MRTCs would make the HIPAA breach notification provisions apply to PMs, even those already subject to HITECH-required breach notification provisions that already require notification to individuals and to the FTC (in the case of larger breaches) and are enforced by the FTC. While we understand the desire to create a "level playing field" with respect to breach notification, **doubling up on breach notification obligations makes no sense and does not result in greater public accountability. It is absolutely not true that the FTC requirements are "weaker" than those for HIPAA.** Entities subject to the FTC breach notification obligations already are required to notify individuals, with a notice that includes the same details as is required in the HIPAA notice. The definition of "breach" in the FTC rules is more tailored to consumer-controlled records – a breach involves access to identifiable information without the authorization of the individual – vs. the HIPAA definition of breach, which is much more tied to whether the access was or was not authorized by the HIPAA rules (which permit disclosures for a number of routine purposes without the need to obtain individual authorization). **Requiring consumer-facing apps, who are not regulated by HIPAA, to report breaches to HHS makes no sense, as HHS has no authority to further investigate these breaches or to impose any penalties. The FTC, under its authority to crack down on unfair and deceptive trade practices, already requires reporting of larger breaches and can investigate and penalize entities who fail to report and fail to adopt reasonable security safeguards.**[8] Because breaches can happen even to entities who prioritize privacy and security safeguards (after all, OCR investigates all larger breaches and closes the overwhelming number of those investigations with no allegations of noncompliance and no further action required), this excessive breach notification is unnecessary and could frustrate the widespread participation by consumer-facing apps in the TEF. **We urge ONC to instead apply breach notification requirements to PMs who are not already covered by the FTC HITECH breach notification rules.** To account for the possibility that Congress could establish more overarching breach notification requirements that apply across a broader spectrum of companies, this requirement could be phrased as requiring compliance with either HIPAA or applicable federal breach notification law.

We also note that Participants (Section 7.12) and Participant Members (Section 8.12) are required to notify other Participants and Participant members who are "directly affected" by a breach. ONC should provide further clarification on what it means to be "directly affected." One example is if the breach triggers a legal notification requirement that applies to the entity (or entities); another is if a breach has occurred and there is uncertainty with respect to which entity caused or experienced the breach and has the notification requirement (so a number of entities feel the need to report in order to be in compliance with the law). However, a breaching entity should not otherwise have to notify entities who provided the data or may have been part of the data "chain" but were not actually involved in the breach. If there is a serious security issue that requires attention, that should be covered as a serious security incident report – which should be reported broadly (to enable all relevant parties in the TEF ecosystem to take effective action), but should not be handled as a "breach" report, as this creates unnecessary exposure of personal data (for those individuals whose data were part of the breach.

The TEFCA makes clear that QHINs, Ps, and PMs can use their own forms to facilitate Individual Access Services. **While we understand that it has long been OCR's position that covered entities could use their own forms to exercise the Individual Right of Access, we urge ONC to eliminate this language in the TEFCA and instead require the RCE to work with QHINs to develop a common HIPAA-compliant form, or**

[8] Although critics of the FTC breach notification rule point to the steeper OCR penalties imposed (and settlements reached), OCR recently adopted much lower caps on its penalty authority (except in cases of uncorrected willful neglect, and FTC commonly imposes 20 year consent decrees in resolving its cases. https://s3.amazonaws.com/public-inspection.federalregister.gov/2019-08530.pdf

require acceptance of any form that meets HIPAA and/or HITECH requirements.[9] The OCR guidance was initially set forth when most covered entities (particularly providers) kept paper records, and the consumer demand for health information was very low. In our experience, most individuals seeking their records – if they have a serious illness – will have at least 4 or more providers from whom they need records. If the TEFCA allows each link in the chain to have their own form, imagine the paperwork nightmare this creates, even for EHI access. Arguably, insistence on one's own form does create a burden to the individual's exercise of his or her right of access, particularly in the digital age. OCR should eliminate this old saw at its next opportunity – but in the meantime, ONC doesn't have to incorporate this relic into the TEFCA.

Finally, we note that the MRTCs require entities participating in the TEFCA – including consumer-facing apps – to identity proof their members/users at IAL2. **We understand and appreciate the need for strong identity assurances. But the description of IAL2 in the TEFCA raises questions about consumer-facing apps, particularly those not connected to a portal or API, will be able to demonstrate IAL2.** It requires any two of the following:

- physical comparison to legal photographic identification,
- comparison to information from an insurance card that has been validated with the issuer, and/or
- comparison to information from an electronic health record (EHR) containing information from prior encounters

Consumer-facing apps establish relationships with users remotely. As an example, Ciitizen might only be able to meet one of these requirements (physical comparison to legal photographic identification), as we do not currently collect or verify insurance cards (as we are not seeking records from payers at present), and we do not have any electronic health record information from new users (we obtain this information only after an individual access request has been fulfilled). We currently require our users to submit a copy of a valid photo id, to digitally sign (through a signature pad) their HIPAA access request forms, and to identify the locations where they've received care and the approximate dates of service (or a date range within which they wish to obtain records, often a 10-year or more span for individuals seeking to compile a comprehensive medical history where they have frequently been seen at the same institutions or practices). To date this has largely been sufficient to enable us to collect full medical records (beyond what is available through portals or APIs) for our beta users. To meet the requirements above would require collection of additional sensitive information from our users, increasing their privacy risks. **We request ONC to provide further clarity on how consumer-facing apps, whose relationships with individuals are made virtually, can meet IAL2 requirements.**

Finally, we note the inclusion of a right of the individual to a summary of disclosures from entities participating in the TEF. In general, Ciitizen supports this and believes it could be one of the most appropriate use cases for the application of the HITECH changes to the HIPAA accounting for disclosures regulations. However, we have concerns that the requirements of the content for this summary include information that might not be automatically collected by the technology facilitating the query-request, or the push, which means hand entry of additional information, making this compliance with this right much more burdensome. We also note that the exceptions match the current HIPAA Privacy Rule Accounting for

[9] HIPAA does not require that individuals submit individual access requests in writing, but covered entities are permitted to do so. HITECH, however, made clear that for individual seeking to exercise their right of access to have information delivered directly to a third party designee, that request had to be in writing and is "clear, conspicuous, and specific." (Section 13405(e).) Arguably in cases where the individual is seeking to have information delivered to a third party, such as an app, a form that meets the HITECH requirements should be sufficient.

Disclosures requirements, which are tailored to covered entities and not really applicable to consumer-facing apps.

Additional Concerns/Comments

Sections 2.2.2, 7.2, and 8.2 of the draft TEFCA allows QHINs, Participants, and Participant Members to retain, access, use and disclose EHI received via the TEF only for certain purposes. This section does not make clear whether this is limited to EHI that was received by a TEF participant (QHIN, P or PM) as the ultimate destination for the EHI (likely not the case for a QHIN) or whether every link in the chain can retain EHI that it was only able to access because it participated in facilitating the transmission of the EHI to the ultimate destination. We have concerns generally about TEFCA being positioned as a vehicle for enriching participants' health information databases – and in particular we have concerns about such data enrichment that occurs because an individual was seeking to exercise their HIPAA Right of Access. **Information received by a QHIN, Participant, or Participant Member in order to fulfill Individual Access Services should be passed on to its destination (the individual or the individual's app, as directed by the individual) and not retained or held by any other link in the chain for any longer than is necessary to assure the access request has been honored. OCR should clarify that when TEF participants serve as conduits for information, they are not permitted to retain or otherwise access, use and disclose this information for any purpose but to facilitate payload delivery.**

We fully support how this revised draft TEFCA handles the federal and state law consent requirements, placing the obligation on the entity subject to the consent law to obtain the consent prior to releasing information. This assures that those with legal obligations to procure consent prior to sharing data fulfill their obligations – but without perpetuating those responsibilities on those without consent legal obligations and potentially creating issues for sharing of information with individuals pursuant to a Right of Access request (which ordinarily shouldn't be subject to a particular consent requirement, but this has been a source of confusion for dataholders) or constraining the ability of individuals to subsequently share their own health information as they choose. We question whether the use of security labeling (such as DS4P) makes sense here, and we submitted comments as part of the proposed interoperability rules questioning the maturity of these standards for widespread use. We would prefer ONC explore use of the TEF to test the robustness and utility of privacy flagging – such as by working with a select QHIN or a few Participants – prior to mandating more widespread use.

Finally, we note in Section 2.2.12 that if a Common Agreement is terminated due to material breach, there is a requirement for the party to destroy all EHI. Setting aside the difficulties of separately storing and maintaining EHI acquired through participation in the TEF (which could be significant), we also question why this would apply to a consumer-facing app, which may be forced to cease participation in the TEF due to material breach of the Common Agreement, but the consumer may not necessarily have terminated his or her relationship with the app. **We see no reason why the consumer should not be allowed to keep data acquired through his or her HIPAA Right of Access.**

Meaningful Choice - Assuring Individuals Who Opt-Out of QHIN Exchange Can Still Exercise the Right of Access

Sections 2.2.3, 7.3, and 8.3 of the MRTCs requires TEF participants (QHINs, Ps, PMs) to provide individuals with meaningful choice regarding exchange of their EHI through the TEF. **We urge ONC to make clear that individuals are able to opt-out for all of the Permitted Purposes except Individual Access Services (i.e., individuals should be able to leverage the TEF to obtain their data without having to agree to more widespread sharing through the TEF).**

Special Category of HIN for Consumer-Facing Apps

In our comments to the prior version of the TEFCA, we urged ONC to adopt tailored rules for consumer-facing apps. As so many of our comments above indicate, we continue to see areas where consumer-facing apps need distinct treatment from other Participant Members or Participants. Again we suggest ONC rely on the definition of "personal health record" from HITECH to help draw a distinction between consumer-facing apps and industry stakeholders leveraging the TEF.[10]

Conclusion

Ciitizen Corporation believes the efforts of ONC in creating the TEFCA are critical to empowering individuals to easily access their health information from wherever in the country they received treatment. We strongly support these efforts and appreciate the opportunity to provide comments intended to strengthen the ability of the TEFCA to serve the needs of individuals and their caregivers.

Sincerely,

Deven McGraw
Chief Regulatory Officer

[10] Term "personal health record" means an "electronic record of PHR identifiable health information (as defined in section 13407(f)(2)) on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual." This is distinct from an "electronic health record," which is information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff. HITECH also made clear that such personal health records would only be "HIPAA business associates" in circumstances where a personal health record is offered to patients "as part of" an electronic health record" (see Section 13408 of HITECH).