Request for Information Regarding the Nationwide Health Information Network: Conditions for Trusted Exchange

June 29, 2012

Steven Posnack
Director, Federal Policy Division
Office of Policy and Planning
Office of the National Coordinator for Health IT
U.S. Dept. of Health and Human Services

Dear Mr. Posnack,

The Center for Democracy & Technology ("CDT") is a non-profit Internet and technology advocacy organization that promotes public policies that preserve privacy and enhance civil liberties in the digital age. As information technology is increasingly used to support the exchange of medical records and other health information, CDT, through its Health Privacy Project, champions comprehensive privacy and security policies to protect health data. CDT promotes its positions through public policy advocacy, public education, and litigation, as well as through the development of industry best practices and technology standards. Recognizing that a networked health care system can lead to improved health care quality, reduced costs, and empowered consumers, CDT is using its experience to shape workable privacy solutions for a health care system characterized by electronic health information exchange.

CDT is frequently relied on for sound policy advice regarding the challenges to health privacy and security presented by health information technology (health IT) initiatives. We have testified before the U.S. Congress five times since 2008 on the privacy and security issues raised by health IT, and we chair the privacy and security policy working group of the federal Health IT Policy Committee (called the "Tiger Team").

The National Partnership for Women & Families is a nonprofit, nonpartisan organization that uses public education and advocacy to promote access to quality health care, fairness in the workplace, and policies that help women and men manage the dual demands of work and family.

CDT submits these comments, on its own behalf and on behalf of the National Partnership for Women & Families, in response to the May 15, 2012, Request for Information (RFI) issued by the Department of Health and Human Services (HHS) Office of the National Coordinator (ONC) regarding the establishment of a of a governance mechanism for the Nationwide Health Information Network (NwHIN),[1]

[1] HHS Office of the National Coordinator for HIT RFI, "Nationwide Health Information Network: Conditions for Trusted Exchange." Fed. Reg. Vol. 77, No. 94, accessed at https://www.federalregister.gov/articles/2012/05/15/2012-11775/nationwide-health-information-network-conditions-for-trusted-exchange.

Trust and interoperability are the most important characteristics of a robust environment for health information exchange and should be established through sound governance principles and mechanisms. Health care providers have ethical and legal responsibilities to protect a patient's health data, and they will need some assurance that entities with whom they share patient data will handle that data responsibly and in compliance with the law. Interoperability ensures that data sent by a provider can be understood and appropriately used by the intended recipient.

In general, governance of health information exchange should have the following characteristics:

- Participation
- Transparency
- Representation
- Accountability
- Effectiveness
- Flexibility
- Well-defined and bounded mission.[2]

More specifically, governance of health information sharing should include the following three components:

- Clear goals and objectives;

- Mechanisms and processes for the development, oversight, enforcement and coordination of policies, standards and services; and

- A set of policies, standards and services that are necessary to support the clear goals and objectives intended to be achieved.[3]

The privacy and security regulations promulgated under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) apply to most health care providers and provide a baseline of privacy and security protections for patient data. But HIPAA likely will not provide a sufficient foundation to alleviate the concerns of providers contemplating sharing data with other providers across a network, for at least three reasons:

- The HIPAA Security Rule is scalable and flexible in order to allow different entities to implement risk mitigation strategies in a manner appropriate for their circumstances.[4] Consequently, a provider contemplating sharing health data with other providers may not have a high degree of confidence in the extent of security precautions adopted by intended data recipients.

---

[2] The Markle Foundation, Policies in Practice: Governance of Health Information Sharing Efforts: Achieving Trust and Interoperability with Meaningful Consumer Participation, accessed at http://www.markle.org/health/markle-common-framework/connecting-professionals/hie-governance (hereinafter Markle Governance Policies).

[3] Id.

[4] Centers for Medicare & Medicaid Services, Health Insurance Reform: Security Standards, FR. 68, No. 34, February 20, 2003.

- Even in circumstances where the HIPAA Privacy and Security regulations set forth specific requirements, varying interpretations of the rules also contribute to reluctance to share data beyond institutional boundaries.

- The business entities that will facilitate the sharing of information from one provider to another will be covered by HIPAA regulations only as business associates. The Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) requires business associates to comply with the HIPAA Security Rule, but the parameters for data sharing between covered entities and business associates are largely defined by the terms of their contracts or business associate agreements. As a result, providers seeking to exchange information through transactions that involve one or more intermediaries are potentially releasing patient data to entities whose data practices are not known.

It will not be possible to give providers 100% assurance that the other providers with whom they share patient information will not breach or misuse that data. Consequently, it will be critical for NwHIN privacy and security governance conditions to focus on provider concerns about data sharing across a network that can be reasonably addressed through a set of additional NwHIN governance conditions.

With respect to interoperability, the electronic health record (EHR) meaningful use and certification requirements mandate the use of certain baseline standards for the exchange of certain types of health data. However, there will need to be a process in place for piloting and implementing new standards - and retiring older, out-of date standards - that is more efficient than relying disproportionately on traditional government rulemaking processes.

We applaud ONC for issuing this RFI at a critical juncture in our national efforts to promote the widespread adoption of HIT to improve individual and population health. Our response to the proposed CTEs, and most of the specific questions asked by ONC in the RFI, are below. We note below those questions for which we do not have specific guidance to provide.

A. Establishing A Governance Mechanism

Question 1: *Would the governance categories (Safeguards, Interoperability and Business Practices) comprehensively reflect the types of CTEs needed to govern the nationwide health information network? If not, what other categories should we consider?*

The Markle Foundation's Connecting for Health Initiative recently released a policy guide on the topic of governance that strongly recommends governance be established to specifically accomplish a set of clear and comprehensible policy objectives.[5] We agree. The health information exchange objectives required to be met by providers participating in Stages 1 and 2 of the HITECH EHR incentive program provide a starter set of policy objectives to be potentially achieved by NwHIN. The initial phase of NwHIN governance

[5] Markle Governance Policies, supra note 2.

should focus on the minimum requirements needed to address specific trust and interoperability concerns that could be obstacles to exchange across the network for Stages 1 and 2. The currently proposed CTE categories – Safeguards, Interoperability, and Business Practices - reflect the types of CTEs needed to initially govern the NwHIN.

Questions 2 and 4*: What kind of governance approach would best produce a trusted, secure, and interoperable exchange nationwide? Are there other approaches ONC should consider? Would a voluntary validation approach as described in the RFI achieve this goal?*

When baseline legal standards are in place to protect data, we endorse the use of voluntarily adopted standards and best practices as an appropriate mechanism for achieving a more trusted environment for information exchange.[6] In the case of exchange among providers, these baseline legal protections are provided by HIPAA and, where applicable, state law. The NwHIN CTEs should be intended to establish a set of model best practices that build on this existing baseline.

Question 3*: How urgent is the need for a nationwide governance approach for electronic health information exchange? Why should ONC exercise its statutory authority to establish a governance mechanism now?*

Providers participating in the EHR incentive program are already faced with requirements to exchange health information, and more robust exchange requirements are expected in Stage 2, which will begin in 2014. In addition, a trustworthy, interoperable exchange environment is critical to implementation of health reform initiatives. We support the efforts of ONC to engage in a vigorous public comment process, in order to ensure that governance conditions are set at the right level, but it will be critical to continue to prioritize this work so that a trusted exchange ecosystem is in place as soon as reasonably possible.

Question 5: *Would establishing a national validation process as described in the RFI effectively relieve any burden on States to regulate local and regional health information exchange markets?*

A national validation process would relieve some but not all of the burden on the states to regulate local and regional health information exchange markets. States will always want the prerogative to tailor exchange initiatives to the unique needs of their residents. Instead of fully relieving state's burden, a validation process would set a consistent framework for states to follow, while allowing states the flexibility to tailor policies within that overall framework to their specific circumstances. Further, it could help prevent states from enacting governance conditions that conflict or are not in sync with federal conditions.

---

[6] Testifying before Congress, Director of CDT's Consumer Privacy Project, stated, "The voluntary, multistakeholder approach offers an open, transparent forum for good faith negotiations among industry, advocates, and regulators. The codes will not be written in stone and will be open to innovation over time." *Brookman Testifies on Administration's Privacy Protections*, https://www.cdt.org/testimony/brookman-testifies-administrations-privacy-proposal.

***Question 6**: How could we ensure alignment between the governance mechanism and existing State governance approaches?*

We acknowledge that one potential weakness of a voluntary governance system is its inability to force alignment between the nationwide governance mechanism and existing State governance approaches. To further promote alignment, ONC could make compliance with NwHIN CTEs a condition of receipt of funding (and more widespread adoption could be achieved if this condition were adopted by other funding agencies within HHS). States should also be part of the process established to update governance conditions as health information exchange matures.

However, some variation in policy among states may be necessary to build trust, because states will need to respond to the needs of their constituents. Such variation need not create obstacles to exchange, as entities seeking to exchange information need only comply with their own state laws and not those of states where they are sending the data.

***Question 7**: What other approaches to exercising our authority to establish a governance mechanism for the nationwide health information network should we consider?*

[We have no specific guidance to offer with respect to Question 7.]

B. Actors and Associated Responsibilities

***Question 8**: ONC seeks feedback on the appropriateness of ONC's role in coordinating the governance mechanism and whether certain responsibilities might be better delegated to, or fulfilled by the private sector.*

We agree with the HIT Policy Committee's governance workgroup that ONC has a critical role to play in NwHIN governance. ONC should play a leading role in promulgating specific policies and standards for NwHIN and for having oversight of NwHIN. Specifically, ONC should:

- Endorse and adopt CTEs and publish guidance;
- Facilitate input from/to the HIT Policy and Standards Committees on revisions to CTEs, creating new CTEs, and retirement of CTEs;
- Select, manage and oversee the an accreditation body that will have oversight over the validating bodies;
- Provide overall oversight of all entities and processes established as part of NwHIN governance.

We believe it is appropriate for ONC to delegate certain responsibilities to the private sector, as long as such delegation is done in a way that is transparent and maintains the trust of stakeholders and the public. With respect to the adoption of standards, we believe ONC should continue to adopt standards for NwHIN, in order to ensure such standards continue to meet the basic technology principles adopted by the HIT Standards Committee (see response to question 60 below). The private sector has a

significant role to play in developing and piloting potential new standards, and for ensuring innovation for existing standards. ONC can leverage NwHIN and other stakeholder groups as standards innovation laboratories to inform the standards adoption process.

Question 9*: Would a voluntary validation process be effective for ensuring that entities engaged in facilitating electronic exchange continue to comply with adopted conditions for trusted exchange (CTEs)? If not, what other validation processes could be leveraged?*

We support the voluntary validation system proposed in the RFI. Establishing accreditation and validation standards upon which consumers, participants, and clients of NVEs can rely is critical. However, the CTEs will not be effective unless there is a mechanism to ensure accountability for complying with them.

The NwHIN governance process should be designed to respond to the unique policy objectives sought to be achieved by NwHIN. Entities that serve validation roles for other purposes might be able to be leveraged for validating NVE status, depending on the skills and expertise needed to assure competent validation.

Question 10*: Should the validation method vary by CTE? What methods would be most effective for ensuring compliance with CTEs?*

We believe the validation method will need to vary by CTE. Some CTEs should be validated through audit or conformance testing (such as implementation of HIPAA Security Rule requirements and use of a required technical standard); others will require examination of NVE policies and audit of whether such policies are being adhered to (such as the requirements regarding meaningful choice). Validators will need to develop the necessary processes to assure NVE compliance with all conditions; it's also possible that validators could specialize in validating a particular type or set of CTEs (and in such a case, an NVE might need to be validating by more than one entity in order to ensure compliance with all applicable CTEs).

Question 11*: What successful validation models or approaches exist in other industries that could be used as a model for our purposes in this context?*

[We have no specific guidance to offer with respect to Question 11.]

Question 12*: What would be the potential impact of this accreditation/validation body model on electronic health information exchange, in particular, on the volume and efficiency of exchange in local health care markets and provider confidence? What is the best way to maximize the benefit while minimizing the burden on providers or other actors in the market?*

There will need to be a sufficient number of accreditors and validators to ensure that the validation process does not become a bottleneck for establishing NwHIN as a trusted environment for exchange. Because NwHIN validation is a voluntary process, the business model for sustainability of the accreditation/validation model is unclear. There

will need to be sufficient resources to ensure both robust accountability as well as sufficient "supply" of validating entities to meet demand.

As noted further below, NVEs should initially be validated for a two-year term. Subsequent validation for the same CTEs could be through a more streamlined process.

C. Entities Eligible for Validation

Question 13*: Should there be an eligibility criterion that requires an entity to have a valid purpose (e.g., treatment) for exchange health information? If so, what would constitute a "valid" purpose for exchange?*

Today health information is collected, stored, used and shared by an increasingly broad range of stakeholders for a wide variety of purposes. Some of these entities qualify as health care providers or health plans covered by the Privacy and Security Regulations of HIPAA; others (particularly those that provide products and services directly to consumers) are not subject to HIPAA protections. Consequently, it will be difficult – if not impossible – to create a set of CTEs that will be appropriate for all types of health information exchange. In addition, privacy and security policies are most effective when they are tailored to the particular context of data sharing. Entities that support consumers in sharing their health data with providers and others could be subject to one set of conditions; these conditions would likely be insufficient to build trust in data sharing among providers or between providers and health plans. Some of the CTEs in the RFI arguably could be applied to a range of purposes (for example, the safeguard CTEs dealing with data security and transparency). However, other CTEs – such as those applicable to patient query capabilities – might be appropriate to apply only to query models of exchange.

The concept of NwHIN governance – and a set of conditions that are layered on top of existing law – is quite new and untested in this environment. Rather than trying to build a trusted ecosystem that is designed to adequately support all types of health information exchange, ONC should utilize a staged approach, initially targeting governance to those entities that facilitate the exchange of health information to enable providers to the requirements of the HITECH EHR incentive program. For the most part, the CTEs identified in the RFI are the right set of starter CTEs for supporting health information exchange among providers for Stages 1 and 2 of the incentive program (exceptions are noted below). If this focused governance effort is successful, ONC can then seek public input on how to scale it to address other health information exchange scenarios.

Question 14*: Should there be an eligibility criterion that requires an entity to have prior electronic exchange experience or a certain number of participants it serves?*

No. NVEs should be required to be transparent about their experience, their years of operation, and the number of participants they serve. This information can then help providers, consumers and other appropriate exchange participants make choices among NVEs.

***Question 15**: Are there other eligibility criteria we should consider?*

In the RFI, ONC notes that it is considering making it a condition of eligibility that an NVE "not have had civil monetary penalties, criminal penalties, or damages imposed, or have been enjoined for a HIPAA violation (by HHS, the Department of Justice, or State Attorneys General) within two years prior to seeking validation."[7] The HIT Policy Committee Governance and Information Exchange workgroups expressed concerns that this language was vague (particularly with respect to the phrase "enjoined for a HIPAA violation") and could result in an entity being barred from being an NVE due to the actions of a few bad actors within their organizations.

We suggest that ONC instead create a CTE for NVEs that mirrors language adopted by the HIT Policy Committee regarding whether providers with HIPAA violations should be eligible for an EHR incentive payment (a suggestion also recommended by the HIT Policy Committee Information Exchange workgroup).[8] Entities could not be an NVE if they have been found liable (or guilty) and fined for a significant civil or criminal HIPAA violation within two years prior to seeking validation. (And NVEs found liable – or criminally guilty – of a significant civil or criminal HIPAA violation could be subject to a one or two-year suspension from NwHIN.) As noted in the HIT Policy Committee's recommendation letter on this topic,

- This CTE should be limited to those circumstances where a fine is levied or imposed, and not imposed at the complaint or investigation stage.
- With respect to civil penalties, this CTE should be limited to those instances of willful neglect of HIPAA regulations. (Willful neglect means "conscious, intentional failure or reckless indifference to the obligation to comply with the…provision violated.")[9]
- With respect to criminal violations, this CTE should only apply in the event of entity or enterprise liability (not to circumstances where individuals within the entity are found to be guilty of a criminal violation of HIPAA).

***Question 16**: Should eligibility be limited to entities that are tax-exempt under Section 501(c)(3) of the Internal Revenue Code (IRC)?*

Restricting NVE status to 501(c)(3) IRC non-profits seems arbitrary. Any lawfully organized entity that is appropriately validated to meet the CTEs should be able to be an NVE.

D. Stakeholders

***Question 17**: What is the optimum role for stakeholders, including consumers, in*

---

[7] U.S. Health and Human Services Department, Request for Information on Nationwide Health Information Network: Conditions for Trusted Exchange, May 15, 2012, 77 FR 28543, 28551.
[8] HIT Policy Committee recommendation letter of March 5, 2010. http://healthit.hhs.gov/portal/server.pt?open=512&objID=1815&parentname=CommunityPage&parentid=37&mode=2&in_hi_userid=11673&cached=true
[9] 45 C.F.R. § 160.401 and .404; see 75 F.R. 40876.

governance of the nationwide health information network? What mechanisms would most effectively implement that role?

We believe it is vital to have broad stakeholder and strong consumer representation on any body that develops policies and standards for NwHIN. If there is to be an overall governing board for NwHIN (either now or in the future), consumers should be represented on that board. Consumers should also have representation on the governing board of any NVE whose operations are supported with taxpayer funds.

E. Monitoring and Oversight

***Question 18**: What are the most appropriate monitoring and oversight methods to include as part of the governance mechanism for NwHIN? Why?*

Reasonably frequent validation is the most appropriate way to monitor and oversee compliance with NwHIN CTEs. (See below – we suggest validation every two years.) Self-attestation without validation does not provide sufficient accountability to build and sustain trust in NwHIN.

Revocation of validation should be the ultimate penalty for failure to comply with CTEs, or misrepresentation of compliance with CTEs. When an NVE fails validation with respect to one or more CTEs, there should be a probationary or provisionary penalty, with a predetermined time in which the NVE must resolve its issues or risk revocation.

Oversight of NwHIN should also include a confidential process for filing complaints about an NVE, as well as a process for dealing with grievances and managing disputes among NwHIN stakeholders. ONC should establish and oversee this process, but potentially could ask a private sector entity to execute and manage it.

***Question 19**: What other approaches might ONC consider for addressing violations of compliance with CTEs?*

[We have no additional guidance to offer with respect to Question 19.]

***Question 20**: What limits, if any, would need to be in place in order to ensure that services and/or activities performed by NVEs for which no validation is available are not misrepresented as being part of an NVE's validation? Should NVEs be required to make some type of public disclosure or associate some type of labeling with the validated services or activities they support?*

NVEs should be required be transparent about which of their particular services are subject to validation (and of those, which have been validated and which have not (if applicable)). At a minimum, such information displayed prominently on the NVE website. NVEs making misrepresentations about validation should be subject to sanctions.

***Question 21**: How long should validation status be effective?*

Validation status should last for two years. ONC should require prompt validation of new or modified CTEs. Validation after the first two years for pre-existing CTEs could be

structured as a simpler, less time-consuming process (a simple check to see if standards are still in place versus full compliance testing, for example). ONC also could consider allowing longer validation periods for policies or technical functionalities expected to be in place for longer periods of time. NVEs making significant changes to a policy, procedure or technical specification relevant to compliance with a CTE could be required to request re-validation of that CTE.

F. Conditions for Trusted Exchange

1. Safeguard CTEs

***Question 23**: Proposed Safeguard-1 (S-1) requires NVEs to comply with sections 164.308, 164.310, 164.312, and 164.316 of the Security Rule as though an NVE were a covered entity and treat all implementation specifications as required. Are there other security frameworks or guidance we should consider for this CTE? Should we look to leverage NISTIR 7497 Security Architecture Design Process for health information exchanges?*

We agree that requiring NVEs to implement all of the HIPAA Security Rule Implementation Specifications will help resolve the concerns driven by the Security Rule's historic flexibility. Such an approach provides more certainty to providers and NVEs seeking to exchange across the network. Over time, ONC could look to strengthen the security protections of NwHIN by leveraging other security frameworks used to support electronic health information exchange. We are not sufficiently familiar with NISTIR 7497 Security Architecture Design Process to comment on whether it should be leveraged for health information exchanges.

***Question 24**: Proposed S-2 provides that NVEs should only facilitate electronic health information exchange for parties it has authenticated and authorized, either directly or indirectly. What is the most appropriate level of assurance an NVE should look to achieve in directly authenticating and authorizing a party for which it facilitates electronic exchange?*

We agree with the Policy Committee's recommendation that providers seeking remote access (such as through the Internet) should be subject to two-factor authentication. NVEs should be responsible for identity proofing and authenticating the sending and receiving entities, and these entities should retain the responsibility for identity proofing and authenticating individual users. The HIPAA Security Rule already requires providers to appropriately identity proof and authenticate users.[10]

However, at the HIT Policy Committee where workgroup recommendations to the RFI were considered, the view was expressed that relying on entities/organizations to appropriately identity proof and authenticate individual users in accordance with their own policies would not be sufficient to create a trust foundation for exchange. The Tiger Team has agreed to pursue this issue further, and to explore how the National Strategy for Trusted Identities in Cyberspace can be leveraged to create a trusted identity

[10] 45 C.F.R. 164.308 and 164.312.

ecosystem for exchange by providers and patients using NwHIN. We look forward to actively participating in those discussions.

Question 25: *Re: S-2 Would an indirect approach (e.g., permitting an NVE to allow its participating organizations to authenticate individual users) reduce the potential trust that an NVE could provide?*

See answer to Question 24.

Question 26: *Re: S-2 and other safeguard CTEs, should ONC consider applying the "flow down" concept (imposing requirements on NVEs that they then just enforce on the parties for which they facilitate electronic exchange)?*

See answer to Question 24.

Question 27: *Proposed S-3 requires NVEs to ensure that individuals are provided with a meaningful choice regarding whether their individually identifiable health information (IIHI) may be exchanged by the NVE. Does accommodating various meaningful choice approaches (opt-in, opt-out, or some combination of the two) pose operational challenges? How could meaningful choice be validated under each approach? Given that some states have already established choice policies, how we can ensure consistency in implementing this CTE?*

We endorse the recommendations of the Tiger Team (ultimately adopted by the HIT Policy Committee) on this issue, [11] although we have some further thoughts on those recommendations (largely in response to issues raised in the HIT Policy Committee's consideration of the RFI on June 6, 2012). As noted in the RFI, consent is meaningful when it:

- Allows the individual advanced knowledge/time to make a decision;
- Is not compelled, or is not used for discriminatory purposes;
- Provides full transparency and education;
- Is commensurate with the circumstances; and
- Is consistent with reasonable patient expectations for privacy, health, and safety; and revocable.

Consistency in approach—opt-in or opt-out—is not as important as meeting these specific criteria, which should also be the basis for validation. Any particular NVE is only required to apply consent with respect to the data sharing it performs or facilitates; consequently, some variation in policy among NVEs is acceptable (and may be necessary in order to accommodate different community norms).

[11] Health IT Policy Committee, A Public Advisory Body on Health Information Technology to the National Coordinator for IT. Recommendations, Sep. 01, 2010. http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_0_6011_1815_17825_43/http%3B/wci-pubcontent/publish/onc/public_communities/_content/files/hitpc_transmittal_p_s_tt_9_1_10.pdf

We agree that additional consent (beyond what might already be required by law) should not be required as a CTE when an NVE is merely facilitating secure, directed exchange (which we understand is the scenario envisioned by Interoperability CTE I-1). Such secure, directed exchange can be initiated by the data holder, or can be pushed by the data holder in response to a request (query) for information.

However, when the decision regarding whether or not to share a patient's health information is no longer in control of the patient's provider (or the provider's Organized Healthcare Delivery Arrangement or OHCA[12]), the patient should have meaningful consent about whether or not his/her information is collected, used, or disclosed by the NVE. Examples of NVEs that should provide meaningful consent include centralized databases, federated models where the NVE controls data sharing decisions, or NVEs that aggregate data from multiple sources. When the NVE model is one where consent should be required, patient should have meaningful consent even if the purpose for exchange is for treatment. The RFI suggests that any exchange for treatment would be exempt from the CTE requiring meaningful choice; such a provision would not be consistent with the Tiger Team and Policy Committee's original recommendations on meaningful choice and is inconsistent with the principle that the patient should not be surprised about what happens to their personal health information.

***Question 28**: Given that the Policy Committee set forth recommendations on choice that apply to exchanges of IIHI for Stage 1 of Meaningful Use, under what circumstances and in what manner should individual choice be required for other electronic exchange purposes?*

The Policy Committee's previous recommendations on meaningful choice were intended to apply to exchange for Stage 1 of the EHR incentive program. We believe these recommendations also can be applied to exchange proposed for Stage 2, which covers similar purposes for exchange (treatment, care coordination, some public health purposes, and reporting of aggregate quality measures to CMS).

In addition, whenever the structure (or architectural model) of the NVE triggers a requirement for meaningful choice, arguably such choice should apply regardless of the purpose for exchange.

We further note that if ONC decides to narrow the scope of the NwHIN to NVEs that support providers meeting their obligations under the EHR incentive program, we see no need to consider whether there are other circumstances where NVEs should be required to obtain meaningful consent (and HIPAA and state law already include consent or authorization requirements for many other uses of IIHI).

[12] An Organized Health Care Arrangement (OHCA) is an arrangement or relationship, recognized in the HIPAA privacy rules, that allows two or more Covered Entities (CE) who participate in joint activities to share protected health information (PHI) about their patients in order to manage and benefit their joint operations, 45 C.F.R. 160.103; HIT Policy Committee Recommendations, Trigger for Additional Consent, Recommendation 3.2, p. 10, accessed at healthit.hhs.gov/portal/.../tigerteamrecommendationletter8-17_2_pdf.

If the policy objectives to be supported by NwHIN are not clearly defined (and NwHIN governance is required to cover exchange for any lawful purpose), ONC should seek further policy guidance on meaningful choice for exchange purposes beyond those required to meet Stages 1 and 2 of the EHR incentive program.

Question 29*: Should an additional meaningful choice safeguards CTE be considered to address electronic exchange scenarios (e.g., distributed query) that do not take place through Interoperability CTE I-1?*

The Policy Committee's recommendations on meaningful choice are triggered in certain types of exchange arrangements, as explained above. When an NVE is structured to enable more direct access by a querying provider – and the decision about whether or not to release the patient's IIHI is no longer vested with the patient's provider/originator of the data, this would trigger choice under current Policy Committee recommendations.

We also believe patients should have meaningful choice about whether their information is included in an NVE patient directory or record locator service.[13]

Question 30*: The process of giving patients a meaningful choice may be delegated to providers or other users of NVE services (as opposed to the patient receiving the choice from the NVE directly). In such instances, how would the provision of meaningful choice be validated?*

The Tiger Team has observed that the relationship between the patient and his or her health care provider is the foundation for trust in health information exchange, particularly with respect to protecting the confidentiality of personal health information. For this reason, we believe that providers should, in most cases, have some responsibility for discussing patient choice with respect to the NVE. Nevertheless, NVEs should also play a role in educating the community about the NVE, its purposes, and its practices, and the NVE should give providers resources to help educate their patients so that meaningful choice is possible. With respect to documentation of consent (when such documentation is needed), in circumstances where providers are responsible for educating patients and documenting consent, meaningful consent can be validated through an attestation from providers. NVEs should periodically audit participants for compliance with meaningful choice requirements.

Question 31*: Proposed S-4 provides that NVEs must only exchange encrypted IIHI. Should there be exceptions to this CTE? If so, please describe.*

We agree that NVEs should only exchange IIHI that is encrypted, or that is transmitted through an encrypted channel. The language of S-4 could be read to require IIHI to always be encrypted, even in cases where the channel for transmission is encrypted. We note, however, that if the HIPAA Security Rule addressable implementation specifications regarding encryption of data in motion are made a requirement for NVEs, CTE S-4 is arguably redundant and can be deleted.

[13] See, for example, Markle Foundation's Common Framework for Private and Secure Health Information Exchange, http://www.markle.org/health/markle-common-framework/connecting-professionals/p3.

***Question 32**: Proposed S-5 requires NVEs to make publicly available a notice of its data practices describing why IIHI is collected, how it is used, and to whom and for what reason it is disclosed. Are there specific uses or actions about which ONC should consider explicitly requiring an NVE to be transparent?*

We support requiring NVEs to make publicly available a notice of its data practices, including why data is collected, how it is used, and to whom and for what purposes it is disclosed. Such notice should be provided to all participants in the NVE (e.g., the individuals for whom the NVE facilitates information exchange) and to consumers and the general public. Notice to the public should be posted prominently on the NVE website; also, NVEs should provide sufficient information to participants to enable them to educate their patients.

As discussed in more detail below, we recommend that NVEs provide such notice for both IIHI and de-identified data.

***Question 33**: Would an NVE be able to accurately disclose all of its activities it may need to include in its notice? Should some type of summarization be permitted?*

We have long advocated for simple and easier to read privacy notices, and a recent report of the Federal Trade Commission (FTC) on protecting consumer privacy similarly recommends that privacy notices/data use policies "clearer, shorter, and more standardized to enable better comprehension and comparison of privacy practices."[14] In order for notices to be short while still being comprehensive with respect to describing data sharing practices, such notices must be

- short, highlighting the most important aspects of data sharing, with an opportunity – such as through website links – for interested individuals to obtain further information; and
- cover common categories of information sharing and not each and every specific instance of data use and disclosure.

ONC could seek further comment or assistance from the HIT Policy Committee in defining standardized categories and terminology for information access, use and disclosure by NVEs.

Notices to patients and/or the public should be written at the reading level of the average patient and in languages commonly used in the community served by the NVE.

***Question 34**: What is the anticipated cost and administrative burden for providing such notice?*

Consistent with the comments of the HIT Policy Committee's Information Exchange working group, we do not believe providing notice will be costly or burdensome if NVEs

[14] Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policy Makers, March 2012, accessed at ftc.gov/os/2012/03/120326privacyreport.pdf.

are permitted to display notice in well-defined categories and if NVEs are provided with a model notice or guidelines.

Question 35*: Should this CTE require that an NVE disclose its activities related to de-identified and aggregated data?*

We believe NVEs should provide notice of its practices with respect to IIHI and with respect to de-identified and/or aggregated data. The notice should be presented in a way that allows the reader to distinguish between uses of IIHI and de-identified data. The notice for each type of data should meet the criteria set forth in the response to question 33 above.

Question 36*: Should this CTE require that an NVE just post its notice on a website or should it be required to broadly disseminate the notice to the health care providers and others to which it provides electronic exchange services?*

See answer to question 33 above.

Question 37*: Proposed S-6 prohibits NVEs from using or disclosing de-identified health information to which it has access for any commercial purpose. What impact, if any, would this CTE have on various evolving business models? Would the additional trust gained from this CTE outweigh the potential impact on these models?*

CDT has been carefully examining federal policies with respect to de-identified health data since 2009, issuing an initial white paper in 2009.[15] This summer, CDT will publish a follow-up article with more specific policy recommendations on de-identified data; it will appear in a special supplement of the Journal of the American Medical Informatics Association. Both CDT and the National Partnership for Women & Families fully appreciate the complexities of crafting policies to govern de-identified data.

Currently under HIPAA, data that meets HIPAA's standard for de-identification is not subject to further regulation, and can be accessed, used, disclosed and/or sold for any purpose. For data to qualify as be de-identified, it must present a "very small"[16] risk of re-identification. However, the risk of re-identification is not required to be reduced to zero – so even de-identified data remains at small risk of being re-identified. Currently federal law does not prohibit re-identification of HIPAA de-identified data; nor is there any redress against those who do re-identify. Entities who use or disclose de-identified data are not required to bind de-identified data recipients to not re-identifying the data (nor are the disclosing entities required to make this commitment).

Further, HIPAA protects the privacy rights of patients and requires de-identified data to carry a very low risk of re-identifying the patient who is the source of the data; HIPAA does not protect the identities of providers. Data that is de-identified as to patients but identifiable as to provider is often used by health product manufacturers for marketing

[15]Deven McGraw, Encouraging the Use of, and Rethinking Protections for De-Identified (and "Anonymized") Health Data, June 25, 2009, accessed at https://www.cdt.org/paper/encouraging-use-and-rethinking-protections-de-identified-and-anonymized-health-data.
[16] 45 C.F.R. §164.514 .

purposes. De-identified data is also used for provide performance measurement as part of quality improvement efforts.

Providers often express concern about the uses of patient de-identified, provider-identifiable data. Concerns have also been expressed about uses of de-identified data for business reasons in ways that end up harming patients or groups of patients. Because uses of de-identified health data are not regulated, we do not have good data on the scope of its uses and disclosures.

We understand the motivation to try to address concerns about uses of de-identified data through proposed CTE S-6, which prohibits the use or disclosure of de-identified data for "any commercial purpose." However, we have the following concerns:

- Sales of de-identified health data have been promoted as a potential model of sustainability for health information exchanges. Prohibiting such activity only by NVEs would not stop such sales but instead could potentially disadvantage NVEs.

- Among the most widespread applications of de-identified data are quality improvement, research (including clinical and epidemiological research), improving the efficiency of operations, and understanding risks to patients. Proposed S-6 could have a chilling effect on existing and emerging business models to support important initiatives.

- It is often difficult in health care to distinguish activities that are purely "commercial" from those that produce revenue and benefit the public. Revenue generating uses of de-identified data also help sustain the infrastructure that allows de-identified data to be used to produce important benefits for the public. Prohibiting commercial uses could have the unintended consequence of shutting down critically important uses of data.

At the June HIT Policy Committee, a number of members floated the idea of barring commercial uses of de-identified data only with respect to data received or transmitted by an NVE through the process of facilitating an exchange transaction, versus trying to impose that regulation on data held by the NVE on behalf of its participants. (In the latter case, the NVE could use or disclose de-identified data with the consent of its participants.) To meaningfully pursue this approach, ONC would have to examine whether it is possible for an NVE to keep separate data the NVE accesses solely to facilitate an exchange transaction. The HIT Policy Committee Governance working group commented that this would be particularly difficult to implement for NVEs who are also providers. Others have suggested that in lieu of barring all commercial uses and disclosures of de-identified data, ONC should instead considering allowing uses and disclosures of de-identified data for purposes of health care operations, research and public health, as those terms are defined in the HIPAA Privacy Rule.

Because of the uncertain impact of this policy on the marketplace for exchange, the sustainability of NVEs, and important initiatives that are conducted with de-identified data, we counsel against pursuing this CTE S-6, particularly in the initial phases of NwHIN governance. Instead, we recommend revising CTE S-6 so that it allows de-

identified data to be used and disclosed by the NVE only:

- Where permitted under the business associate agreement the NVE has with its participants;

- When the NVE publicly commits, in its notices of data practices, not to re-identify de-identified data;

- When uses and disclosures of de-identified data are disclosed in the NVE's public notice of data practices; and

- When the NVE prohibits any downstream recipients of de-identified data from re-identifying it.

ONC should monitor whether this CTE is sufficient to build trust in NwHIN or if further policies on de-identified data are needed.

This approach was recommended by the HIT Policy Committee's Information Exchange workgroup and is consistent with the FTC's recent report on consumer privacy, "Protecting Consumer Privacy in an Era of Rapid Change."[17] In order for data to be de-identified, it should be both consistent with HIPAA de-identification standards and also with the FTC's definition of what constitutes "reasonably de-identified."[18] Of note, the recommended privacy framework promoted by the FTC in the report would not be applicable to data that was reasonably de-identified and protected from re-identification. For ONC to more stringently regulate uses of de-identified data would be inconsistent with this approach to de-identified data.

Finally, ONC should take care not to impose a condition that might not be constitutional, given the Supreme Court's recent decision in Sorrell v. IMS Health Inc. et al. In that case, the Court struck down a Vermont statute that attempted to bar uses of patient de-identified but prescriber identifiable data for pharmaceutical marketing purposes. The Court determined that the statute impermissibly burdened the free speech rights of pharmaceutical companies.[19]

***Question 38**: On what other entities would S-6 have an effect?*

To the extent providers and others depend on NVEs for analysis of de-identified data, they would be impacted by this policy as well.

---

[17] Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policy Makers, March 2012, accessed at ftc.gov/os/2012/03/120326privacyreport.pdf.

[18] According to the FTC report, "the company must achieve a reasonable level of justified confidence that the data cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, computer, or other device," accessed at ftc.gov/os/2012/03/120326privacyreport.pdf.

[19] Deven McGraw, "Lack of Genuine Privacy Interest Doomed Vermont Drug Marketing Law," iHealthBeat, July 11, 2011, http://www.ihealthbeat.org/perspectives/2011/lack-of-genuine-privacy-interest-doomed-vermont-drug-marketing-law.aspx.

Question 39: *What standard of availability, if any, is appropriate?*

[We have no specific guidance to offer with respect to Question 39.]

Question 40: *Proposed S-8 requires NVEs that assemble or aggregate health information that results in a unique set of IIHI to provide individuals with electronic access to their unique set of IIHI. What further parameters, if any, should be placed on what constitutes a "unique set of IIHI"?*

We agree that patients should have the right to promptly access data that is assembled or aggregated by an NVE. Such data may not be available directly from the patient's providers in the form maintained by the NVE. But as part of the Tiger Team and HIT Policy Committee deliberations about this CTE, some expressed concerns about imposing this obligation directly on NVEs, because NVEs often do not have a direct relationship with the patient. In addition, the HIPAA Privacy Rule does enable a provider to withhold information from a patient in rare circumstances, and it would be inappropriate for most NVEs to make these judgment calls. Also, the CTE frames this right in terms of "unique," data, a term that may be difficult to define.[20]

However, we recommend relying on the HIPAA Privacy Rule to develop the parameters for a patient's right to access data held by an NVE.

Under 45 CFR 164.524, patients have the right to access, inspect and obtain a copy of protected health information about them "in a designated record set." (HITECH then made clear patients can get an electronic copy when the data is held electronically.[21]) The term "designated record set" is not limited to information created by the covered entity. It is defined as a "group of records maintained by *or for* a covered entity health care provider…used, in whole or in part, by or for the covered entity, to make decisions about individuals."[22] Business associates obtain data from covered entities in order to perform services on their behalf.[23] Consequently, an NVE creating aggregated or unique data as a business associate is doing so at the direction of, and on behalf of, its covered entity participants. Data that an NVE creates that is used to make decisions about patients is data that a patient has the right to access under HIPAA. Covered entities must permit an individual to obtain or inspect information contained in a designated record set unless one of the rare exceptions applies.

Ordinarily individuals obtain information from a designated record set directly from covered entities, but such entities could, through the business associate agreement, require the NVE to perform this function. If the covered entity does not require the NVE

---

[20] The term "unique data" is not defined in the HIPAA regulations. It has been defined by the NIH to mean data that cannot be readily replicated- such as large-scale studies on disease patterns, or expensive surveys. http://grants.nih.gov/grants/policy/data_sharing/data_sharing_guidance.htm#unique But this definition is not useful for purposes of this CTE.

[21] 13405(e)(1). http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf.

[22] 45 C.F.R. 164.501.

[23] 45 C.F.R. 160.103 (1)

to perform this task, the covered entity is responsible for obtaining it from the NVE. When a covered entity has to obtain designated record set information for a patient from an offsite location, they get some additional time under the rule for producing this record (up to 60 days).[24] We hope, in the digital age and consistent with the direction of the meaningful use requirements with respect to patient access to data, these timeframes could be significantly shortened.

We believe modification or clarification of the Privacy Rule on patient access to designated record set information held by business associates might be a more effective way to ensure patients have access to this information, given the voluntary nature of NwHIN governance. But since such a modification might take some time to accomplish, ONC should maintain this as a CTE.

Question 41*: Proposed S-9 further provides that for NVEs that assemble or aggregate health information that results in a unique set of IIHI, such NVEs must provide individuals with a right to request a correction and/or annotation to this unique set of IIHI.*

Under the HIPAA Privacy Rule, patients also have the right to request amendments or annotations to information in a designated record set, Under the Privacy Rule, the covered entity makes the judgment as to whether or not to accept the requested amendment; the covered entity also has the obligation to forward the amendment (if accepted) to persons, including business associates, that the covered entity knows have the protected health information that is the subject of the amendment, and that may have relied or could foreseeably rely on the information to the detriment of the patient.[25] If the covered entity disputes the requested amendment, and the patient seeks to append information to the record, any further use or exchange of this information must include the patient's appended information (and any rebuttal to the patient's version added by the covered entity to the record).[26]

Since HIPAA provides this right to patients with respect to designated record set data created by the covered entity, this right should extend automatically to business associates (NVEs) who use covered entity data to further create designated record set data (such as aggregations or summaries).

The covered entity is ultimately responsible for complying with HIPAA with respect to amendments to data the covered entity initially creates but then is subsequently aggregated or used by an NVE to create additional information intended for use in making decisions about patients. The covered entity can ask the NVE to fulfill this right on its behalf, or can take responsibility for managing this directly with the patient. Similar to our response to question 41, HIPAA should be clarified to address this circumstance. However, if that cannot occur in a timely way, ONC should retain this CTE as part of NwHIN governance.

[24] 45 C.F.R. 164.524
[25] 45 C.F.R. 164.526(c)(3).
[26] 45 C.F.R. 164.526(d)(5).

This CTE should be expanded to require NVEs to have a process for communicating amendments to data to other covered entity participants of the NVE who have received the disputed data and may rely on it to the patient's detriment.

Question 42: *Re: S-9, are there any circumstances where an NVE should not be required to provide individuals with the ability to correct their IIHI?*

The HIPAA Privacy Rule spells out a clear process for how individual requests for amendment are to be handled;[27] the CTE should require compliance with those rules.

Question 43: *Proposed S-10 requires NVEs to have a means of verifying that a provider requesting an individual's health information through a query and response model has or is in the process of establishing a treatment relationship with that individual. What method or methods would be least burdensome but still appropriate for verifying a treatment relationship?*

We agree that to build public trust in NwHIN, queries of patient data across the network should be limited to those that support treatment of that patient (or, in limited circumstances, treatment of a relative). We note that the RFI is not clear that NVEs that support query models for accessing patient data should limit access across the network to treatment purposes only; ONC should make this clearer in the proposed NwHIN governance rules.

We suggest setting this limit for queries to an NVE from the network (i.e., from providers or patients that are not direct participants in that NVE). The purposes for which data can be queried by a participating entity in an NVE should be a matter of policy collectively set by the NVE and its participants. ONC should also be clear about patient choice requirements with respect to queries to an NVE (see response to question 29).

The least burdensome way to establish that a treatment relationship exists or is in the process of being formed (for example, when information is gathered in advance of a visit,) is to have the provider attest to such a relationship. ONC could consider requiring NVEs to keep reports of who has queried a patient's data, which could be made available to the patient as an oversight mechanism for appropriate attestation. ONC should also consider allowing NVEs to innovate with respect to methodologies for verifying a treatment relationship; however, NVEs should not be permitted to impose verification methodologies that are attempts to exert market power or are so burdensome as to create obstacles to the appropriate access of data.

Question 44: *Re: S-10, are there circumstances where a provider should be allowed through the NVE to access the health information of one or more individuals with whom the provider does not have a treatment relationship for the purpose of treating that accessing provider's patient?*

We agree that it may be necessary to allow providers to access the information of a patient's immediate family members in order to treat a patient, and the NwHIN can be an important tool for accessing this information. As part of the meaningful consent process,

[27] 45 C.F.R. 164.526 et seq.

NVEs that offer a record locator service, or that have an architectural model that triggers meaningful choice can include consent to allowing an individual's information to be accessed for the treatment of family members (blood relatives) as part of the meaningful choice process. Providers seeking this information would then attest to having a treatment relationship with the family member.

2. Interoperability CTEs

***Question 45**: What types of transport methods/standards should NVEs be able to support?*

***Question 46**: If a secure "RESTful" transport specification is developed during the course of this rulemaking should we also propose it as a way of demonstrating compliance with this CTE.*

***Question 47**: Are the technical specifications appropriate and sufficient for the enabling the easy location of organizational certificates? Are there other specifications we should consider?*

***Question 48**: Should this CTE require all participants engaged in planned electronic exchange to obtain an organizational (or group) digital certificate consistent with the policies of the Federal Bridge?*

[We have no specific guidance to offer with respect to Questions 45-48.]

***Question 49**: Proposed Interoperability CTE 3 (I-3) requires NVEs to have the ability to verify and match the subject of a message, including the ability to locate a potential source of available information for a specific subject. Should NVEs be required to employ matching algorithms that meet a specific accuracy level or a CTE that limits false positives to a certain minimum ratio? What should those required levels be?*

Not all NVEs will need to have the capability of verifying and matching the subject of a message. NVEs that facilitate directed exchange from one provider to another do not need to access the content of the message and instead are only responsible for ensuring that the data is routed to the intended recipient. In such cases, the matching will need to be done by the providers at both ends of the transaction (the sending provider will need to send the right patient's data, and the recipient will need to either match the subject of the information (or send the information back or destroy it if the information is not for the right patient). NwHIN CTEs should not drive NVEs to adopt data practices that are not essential to the transactions they facilitate.

For those NVEs that directly receive information on patients, or store patient information in repositories, those NVEs will need to have the ability to verify and match the subject of a message – thus, a CTE requiring this capability is appropriate in those circumstances. We counsel against requiring that matching algorithms meet a specific accuracy level (or be required to limit false positives to a certain minimum ratio). The HIT Policy Committee's Tiger Team held a hearing on patient matching on December 9, 2010; based on the hearing testimony, the Tiger Team concluded (and the Policy Committee agreed) that there is no one-size fits all solution, and that "acceptable margins of error

(false positives and/or false negatives) vary based on the purposes for accessing or disclosing information, populations and settings."[28] We agree with the HIT Policy Committee's Tiger Team, which observed that "data matching is an area of rapid evolution, and establishing and disseminating best practices is more desirable (and achievable) than establishing quantified standards or specific numeric targets." The HIT Policy Committee Information Exchange workgroup, in its response to the RFI, also rejected establishing a universal accuracy level or minimal error ratio for all NVEs.

Consistent with the HIT Policy Committee's previous recommendations on patient matching, we recommend that NVEs needing to perform patient matching functions be required to establish programs to evaluate the efficacy of their matching strategies and to improve their efforts to achieve accuracy on an ongoing basis. NVEs also should have clear policies on how the NVE will respond when information is inadvertently matched incorrectly. ONC also should capitalize on these NVE efforts to develop and disseminate evidence about best practices in improving health data capture and matching accuracy.

ONC could also consider having NVEs report on matching accuracy for common exchange use cases. Such reports could initially be confidential and used primarily to gather evidence about efficacy of algorithms and matching strategies. As a further step, ONC should consider requiring public disclosure of NVE matching results as a mechanism to spur improvement in matching accuracy.

Of note, CTE I-3 states that NVEs should have "the ability to locate a potential source of available information for a specific subject." Some have concluded that this requires all NVEs to establish patient directories or patient record locator services. Since NVE exchange models will vary, they should not be required to establish this functionality. Instead, NVEs who have this capability should be transparent about this service and should abide by the requirements for meaningful choice and other applicable CTEs.

Question 50*: Re: I-3, what core data elements should be included for patient matching queries?*

We agree with previous recommendations of the HIT Policy Committee and its Tiger Team that use of any particular data field should not be required for matching, as choice of fields used to match depends on a number of factors, including the purpose of the data access. Universal identifiers are not a panacea. Instead, ONC should pursue requiring the use of standard formats for data fields (such as demographic data fields) that are commonly used in matching patients to their data, including standard responses for representing data that is unavailable.

Question 51*: Re: I-3, what standards should ONC consider for patient matching queries?*

See responses to questions 50 and 51.

[28] HIT PC recommendation letter of February 8, 2011.

3. Business Practice CTEs

***Question 52**: Proposed Business Practice CTE 1 (BP-1) provides that an NVE must send and receive any planned electronic exchange message from another NVE without imposing financial preconditions on any other NVE. Should this CTE be limited to only preventing one NVE from imposing a financial precondition (such as a fee) on another NVE or should it be broader to cover other instances in which an NVE could create an inequitable exchange environment?*

CDT participated in shaping the comments of the HIT Policy Committee's Information Exchange workgroup on this question. Consistent with the principles of Internet neutrality, NVEs should not be permitted to impose fees or other requirements on NVEs for basic exchange services, including transporting messages from one provider to another and discovering digital certificates. To the extent that NVEs operate like Internet Service Providers, they should not be permitted to impose fees or conditions that obstruct NwHIN access.

However, when an NVE is providing a value-added service to others on the network, they should be permitted to charge fees for those services, as long as the fees are commercially reasonable and are non-discriminatory.

***Question 53**: Re: BP-1, should this CTE (or another CTE) address the fees an NVE could charge its customers to facilitate electronic exchange, or should this be left to the market to determine?*

Fees that an NVE charges to its customers should be left to the market to determine.

***Question 54**: Re: BP-1, under what circumstances, if any, should an NVE be permitted to impose requirements on other NVEs?*

As noted in the response to question 52, when an NVE is providing a set of services beyond facilitating basic NwHIN connections to enable exchange, they should be permitted to charge fees for those services, as long as those fees are commercially reasonable and non-discriminatory.

Comment re: Proposed BP-2, (no specific question asked in the RFI): An NVE must provide open access to the directory services it provides to enable planned electronic exchange.

We endorse requiring NVEs to grant open access to the directory services it provides to enable planned electronic exchange. However, this condition should be limited to 'provider' directories; ONC should carefully consider patient privacy issues before extending this condition to patient directories. (We interpret the term "planned" to refer to directed exchange from one provider to another intended provider recipient.)

***Question 55**: Proposed BP-3 requires NVEs to report on users and transaction volume for validated services. What data would be most useful to be collected? How would it*

be made available to the public? Should NVEs have to report on transaction volume by end user type (e.g., provider, lab, public health patient, etc.).

We agree with the comments of the HIT Policy Committee's Information Exchange workgroup on this question. Requiring NVEs to report transaction volumes to federal and state regulatory agencies (including ONC) is appropriate. Reporting standards should be transparent to both the public and NVEs to ensure their participation. Public reporting should be sufficient to enable evaluation of the progress of national and statewide information exchange, but should not reveal transaction volume or type of transactions facilitated for specific NVEs. Reporting requirements for NVEs should also vary based on the type of services they offer.

G. Request for Additional CTEs

Question 56*: What CTEs would you revise or delete and why? Are there other CTEs not listed here ONC should also consider?*

See response to Question 15.

Question 57*: Should one or more of the performance and service specifications implemented by participants in the Exchange be included in our proposed set of CTEs? If so, please indicate which ones and provide reasons.*

[We have no specific guidance to offer with respect to Question 57.]

Question 58*: Should any of the above CTEs be packaged together for purposes of validation? In other words, would it make sense to allow for validation to different bundles of CTEs for different electronic exchange circumstances?*

Per the comments above, due to the variation in NVE models, we agree that CTEs may need to be bundled or packaged together for purposes of validation.

Question 59*: Should we consider including safe harbors for certain CTEs? If so, which ones and what should the safe harbors be?*

Safe harbors can be particularly effective for those CTEs that provide some flexibility with respect to compliance. Most of the CTEs set forth in the RFI are already fairly specific with respect to NVE compliance; however, for current and future CTEs that provide some flexibility in implementation, safe harbors on how to achieve compliance can be helpful in eliminating uncertainty and creating clearer pathways to validation.

ONC should reach out to the Office for Civil Rights, which enforces HIPAA, and consider whether validation to CTEs that have their foundation in the HIPAA Privacy or Security Rules can serve as a safe harbor for NVEs and their participants with respect to potential HIPAA liability. Compliance with HIPAA is a baseline for providers seeking to exchange patient information, and NVEs will be vehicles for facilitating that exchange (and covered by HIPAA as business associates). To the extent a CTE establishes a best practice for privacy and security, and is in compliance with the HIPAA privacy and security rules, establishing a HIPAA safe harbor for NVEs who are validated to those CTEs would go

along way to reducing concerns about exchange of patient information across the network.

H. CTE Lifecycle

Question 60. *What process should ONC use to update CTEs?*

See our response to question below. We further urge ONC to continue to use the Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information[29] as the overall set of principles guiding policies regarding privacy and security for NwHIN. Those principles include:

- Individual access
- Correction
- Openness and Transparency
- Individual Choice
- Collection, Use and Disclosure Limitation
- Data Integrity and Quality
- Safeguards
- Accountability

Similarly, we urge ONC to continue to adhere to the HIT Standards Committee's Technology Principles in establishing technical capabilities and interoperability standards for NwHIN.[30] Those standards include:

- Keep it simple (standards should be as minimal as required to support a necessary policy objective or business need, then build from there)
- Keep the implementation costs as low as possible
- Don't let "perfect" be the enemy of "good enough" (go for the 80% that everyone can agree on, and focus on the basics before getting to the more obscure)
- Design for the little guy
- Do not try to create a one-size-fits-all standard (e.g., don't add burden or complexity to simple use cases)
- Separate content and transmission standards
- Create publicly available vocabularies and code sets
- Leverage the web for transport
- Position quality measures so they motivate standards adoption
- Support implementers

Question 61. *Should we expressly permit validation bodies to provide for validation to pilot CTEs?*

[We have no specific guidance to offer on Question 61.]

---

29 http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10731_848088_0_0_18/NationwidePS_Framework-5.pdf

30 *http://*healthit.hhs.gov/portal/.../hitpc-standards-update-07-06-11.ppt

***Question 62**: Should we consider a process outside of our advisory committees through which identification and development to frame new CTEs could be done?*

We agree with the HIT Policy Committee Governance workgroup that the HIT Policy and Standards Committees should be the primary vehicles for vetting new CTEs. However, the Committees should not be the only mechanism for generating ideas for new CTEs, or for suggesting modifications to current CTEs. ONC should have an open and transparent process for seeking input from stakeholders on the public, suggestions that can be further vetted through the federal advisory committees.

I. Technical Standards and Implementation Specifications Classification Process

***Question 63**: What would be the best way(s) ONC could help facilitate the pilot testing and learning necessary for implementing technical standards and implementation specifications categorized as Emerging or Pilot?*

***Question 64**: Would this approach for classifying technical standards and implementation specifications be effective for updating and refreshing Interoperability CTEs?*

***Question 65**: What types of criteria could be used for categorizing standards and implementation specifications for Interoperability CTEs? We would prefer criteria that are objective and quantifiable and include some type of metric.*

***Question 66**: ONC encourages comment and citations to publicly available data regarding the potential costs of validation, potential savings to states or others due to establishment of an NVE validation process; potential increase in secure exchange that might result from establishment of CTEs, potential number of entities seeking to become NVEs, and NVE application and reporting burden associate with the proposals in the RFI.*

[We do not have specific guidance to offer for Questions 63-66.]

J. Patients as NVE Customers

We urge ONC to promptly begin work on CTEs that will apply to NVEs that facilitate exchange managed by patients. Those CTEs will be needed to support the proposed Meaningful Use Stage 2 requirements for download and transmit functionalities and the patient's right established in HITECH to have electronic data directly sent to the entity of his or her choice.

ONC should take the lead on developing patient-centered CTEs because patient-facing NVEs will not likely be covered by HIPAA and will need baseline protections in order to protect patient information and build trust in the digital health ecosystem. CDT urges ONC to rely on the Markle Common Framework for Networked Personal Health

Information[31] and the Blue Button Framework[32] in establishing CTEs for patient-mediated exchange.

K. Conclusion

We strongly support ONC in the establishment of a governance mechanism for the Nationwide Health Information Exchange Network. We thank ONC for the opportunity to issue these comments. Please do not hesitate to contact us if we can be of any assistance.

Sincerely,

Deven McGraw
Director, Health Privacy Project
Center for Democracy & Technology

Christine Bechtel
Vice President
National Partnership for Women & Families

[31] http://www.markle.org/health/markle-common-framework/connecting-consumers.
[32] http://www.markle.org/news-events/media-releases/health-it-investments-should-enable-people-download-their-own-information.