S. Arnold Zimmerman, Esq. ("Van"), MBA, CISSP
Privacy & Security Officer
Jersey Health Connect
782 Alexander Road
Princeton, NJ 08543
609.945.3957
van.zimmerman@jerseyhealthconnect.org

Jersey Health Connect ("JHC") is pleased to have the opportunity to comment on Connecting Health and Care for the Shared Nationwide Interoperability Roadmap. We recognize the significant effort that ONC put forth in drafting the Roadmap, and applaud the ONC's efforts towards effecting secure health exchange that appropriately respects patients' privacy.

ONC has provided specific questions to which it is seeking a response in addition to several more open-ended general queries. We have responded to those specific questions first.

1. Question 2-Priority Use Cases. ONC requested comment on three priority use cases from Appendix H that should inform priorities for the development of technical standards, policies and implementation specifications. We put forth the following:

Use case 19. Patients audit their medical records, providing amendments and corrections and supplying missing data such as health outcomes.

The HITECH Act amended the HIPAA Accounting of Disclosure requirements at 45 C.F.R. 164.528, requiring covered entities to account for disclosures made for treatment, payment and health care operations where such were made through an electronic health record. However, regulations implementing these HITECH amendments are still pending. There are also proposed revisions to 45 C.F.R. 170.314(d)(9) (proposed 170.315(d)(9)) relating to Accounting of Disclosure certification criteria for electronic health records under the Medicare and Medicaid EHR Incentive Programs 2015 Edition Health IT Certification Criterion ("2015 CEHRT").

JHC would therefore recommend that the 2015 CEHRT Accounting of Disclosure and related certification criterion are aligned with the HITECH Accounting of Disclosure requirements, such that use of 2015 CEHRT to record disclosures for treatment, payment and health care operations purposes would satisfy a covered entity's obligation to record and account for such disclosures for purposes of HIPAA. For example, changes proposed to the 2015 CEHRT criterion "Activity history log", 45 C.F.R. 170.315 (e)(1)(ii), require the recording of "where applicable, the addressee to whom an ambulatory summary or inpatient summary was transmitted." We would recommend replacing "Where applicable" with stronger language such as "if transmitted" and "the addressee" replaced with "the destination entity or person". We would also request clarification on what "transmitted" means in the context of "addressee." Does "addressee" imply electronic messaging only, such as through DIRECT, or other forms of electronic transmissions?

We note that this use case would require somewhat similar technical capabilities to, at a minimum,Use Cases 40 and 46, so pursuing this Use Case would potentially advance several at once.

Use Case 22. Those who pay for care use standardized transactions and interoperability to acquire data needed to justify payment.

JHC would welcome a standard that incorporates guidance on what data is reasonable and necessary for payment purposes.. For example, health information exchange organizations may wish to broaden participation to include payors. Having "rules of the road" would provide some level of assurance that payors could only acquire data needed to justify payment.

Use Case 56. Individuals exercise their choice for consent and consent management policies and procedures are in place to enable the private and secure electronic exchange of behavioral health data.

Many entities refuse to make behavioral health data available due to the lack of standards around the privacy of such data. This use case would require capabilities which could enable consent management around other types of sensitive care, and if properly leveraged, could both help alleviate some of the issues surrounding the myriad of state rules regarding sensitive information, as well as encourage entities to make such other data available for electronic exchange, rather than withholding it, as is currently done.

2. Question 3- Governance. ONC requested comment on how ONC can best recognize and support the industry-led governance effort. JHC, as one of the largest private health information exchange organizations in the United States, would like to recommend that any governance process that ONC adopts appropriately include and support those private exchanges which have a demonstrated initiative and ability to establish meaningful health exchange, quantitatively and qualitatively, as well as build appropriate governance and sustainability infrastructures.

3. Question 4- Supportive Business, Cultural, Clinical and Regulatory. ONC requested comment on how private health plans and purchasers can support providers to send, find or receive common clinical data across the care continuum through financial incentives, and whether they should align with federal policies that reinforce adoption of standards and certification. JHC would recommend alignment of private payors and purchasers by having requirements aligned with federal policies regarding standards and certification.

4. Question 5-Privacy and Security Protections for Health Information. ONC requested comment on what security aspects of RESTful services need to be addressed in a standardized manner. We believe it is necessary to understand the limitations of RESTful architecture. In particular, it is the protections around those services which are an opportunity for standardization. For example, there could be a standard for securing the transport mechanism to provide those services (even if the standard is provided is a menu of choices). Likewise, there could be a standard for client system authentication when accessing those services.

Within the architecture itself, ONC may wish to consider standards around things such as code on demand, as such functionality is likely to encounter client systems subject to security policies that inhibit that functionality. That, in turn, creates the potential for differing levels of accessibility to a particular system, which would run contrary to interoperability goals. Having to tell a provider or patient "turn down your web security settings in order to access your medical records" would run contrary to establishing trust in health information exchange. Question 6-Core Technical Standards and Functions

JHC believes the approach proposed for Accurate Individual Data Matching is a good starting

point. Data quality is an issue that we find a perpetual challenge. If we assume, for the moment, that data is accurate, we still have an issue regarding matching with another organization - specifically "how much of a match do we need to consider a record as belonging to an individual."

We would note that the roadmap has ONC and SDOs standardizing "additional, required elements for identity matching." It is unclear from the Roadmap when initial required elements for identity matching get standardized, and by whom. Identity matching is critical for meaningful interoperability, and the lack of a standard for what ONC considers to be an acceptable match between a patient and a record is an obstacle for interchange. We would strongly recommend ONC reconsider reprioritizing all of the items in the 2018-2020 timeline in Table 13 for immediate action. We would also recommend that, if SDOs develop those standards, that ONC formally adopt those standards.

5. Question 1-General

There is currently a lack of formal, required standards regarding privacy and consent management. As touched on above, this lack of standards causes some organizations to withhold entire categories of data rather than run the risk of inappropriate disclosure. EHR vendor functionality, or lack thereof, can exacerbate this problem.

ONC should strongly consider formalizing consent criteria for use in restricting use or disclosure of data. Properly implemented that consent criteria could take into account a number of potential uses, such as the basic TPO, but also research, population health, etc., as well as behavioral health. Also, properly implemented such consent criteria could include "flags" for care which implicates state-specific use and disclosure rules, such as for minors who seek treatment for care for which New Jersey deems them emancipated. As an added, such criteria could be used for authorization assertions when one seeks access to data (such as a payor asserting a payment reason for data access). Such assertion could then be used to provide a specific access to appropriate data.

While ONC should consider future certification criteria requiring EHR vendors to implement such a standard (that itself needs to be formally established), such implementation will require those EHR vendors to implement episode-of-care level authorization with respect to data access. ONC should also consider whether there is an opportunity to mandate episode-of-care level consent and access management in the certification criteria, as such is not necessarily dependent on the specific form of consent criteria, just that it exists.