August 25, 2017

National Coordinator for Health Information Technology
Office of the National Coordinator
U.S. Department of Health and Human Services
330 C ST SW
Mary Switzer Building; Office 7009A
Washington, D.C. 20201

RE: Comments Related to a Trusted Exchange Framework and Common Agreement

Dear Dr. Rucker:

The Strategic Health Information Exchange Collaborative (SHIEC) appreciates the opportunity to provide comments to the Office of the National Coordinator for Health Information Technology (ONC) regarding a Trusted Exchange Framework and Common Agreement. In addition, SHIEC is appreciative for the invitation to attend the stakeholder event, hosted by the Office of the National Coordinator (ONC) on Monday, July 24, 2017, and the opportunity to present SHIEC's Patient Centered Data Home ™. SHIEC shares ONC's common goal of achieving nationwide, interoperable health information exchange which ultimately supports effective care delivery and high-quality patient outcomes.

The Strategic Health Information Exchange Collaborative (SHIEC) is the national trade association of health information exchanges (HIEs). Its fifty-four (54), HIE member organizations manage and provide secure digital exchange of health data for hospitals, healthcare providers and other participants approaching more than seventy percent (70%) of the U.S. patient population. As the unbiased, data trustees in their communities, SHIEC member organizations serve a critical role through information exchange with advancing effective, efficient healthcare delivery to improve health on a local, regional and national level. SHIEC's membership expands beyond HIE organizations to include 30 Strategic Business and Technology members and 5 Associate members.

SHIEC's Patient Centered Data Home ™ (PCDH) is a cost-effective, scalable method of exchanging patient data among health information exchanges throughout the country based on triggering episode or care encounter alerts enabling providers to have access to real-time information across state and regional areas and across the care continuum. To date, PCDH has provided over 2.2 million, event notifications exchanged between seventeen (17), health information exchange organizations that serve over 34 million patients living in the PCDH regions.

In this letter, we are providing feedback on the six trust principles which have also been submitted through the ONC comment portal. We support ONC's work to achieve widespread interoperability and commend ONC for seeking industry stakeholder input on this important topic.

A trusted exchange framework should leverage well-defined standards that ensure data accuracy and consistency throughout all exchange activities. We encourage ONC to continue work with industry leaders and experts in defining and refining standards and interoperability criteria as well as identifying preferred standards in areas where multiple standards exist. We recommend that ONC should define the definition of a trusted exchange framework including the criteria or requirements and describe the difference between a network and a framework. We also recommend an approach of using the six principles outlined in this comment period to build upon to develop a slate of guiding principles for a trusted exchange network. The approach leverages the current exchange networks, such as PCDH and health information exchange organization networks, and provides an avenue for their future growth and continued maturity. This slate of *trusted exchange network principles* should include mechanisms to accommodate future user cases and industry requirements, new technologies and future innovations, as well as emerging and non-traditional providers such as social services and community services. The principles would also drive the requirements for future, common agreements for use between data exchange participants.

In addition, we recommend that ONC clearly identify the scope of voluntary compliance and how this is envisioned to work. ONC should evaluate options that avoid disruption of existing exchange network activities and data sharing agreements while minimizing additional work and financial expense for exchange organizations and their provider participants.

Comment Area 1: Standardization

A trusted exchange framework would best be achieved through development and adoption of well-defined standards and the alleviation of multiple standards where more than one standard exists. Having one set of data standards and associated implementation guidelines will increase interoperability and data exchange capabilities across disparate systems and software applications within a single organization and across multiple organizations and geographic regions. A set of clear, well-defined standards will facilitate the efficiency of HIE organizations with exchange activities leading to overall effectiveness with data use and analytic capabilities. Defined standards will limit developers and implementers for the need of customized transactions, remove data incompatibilities and decrease the need for custom interfaces. Flexibility must be maintained with any trusted exchange framework as many new, emerging data sources and use cases evolve which may not have established standards. We encourage ONC to continue their work with supporting development and implementation of effective standards which is critical for operational efficiency within trusted exchange framework.

ONC should consider establishing a clear definition of a trusted exchange network and framework with the associated qualifications. We recognize that achieving this degree of standardization with clinical data is not easy as compared to financial data. To this end, we encourage ONC to leverage industry experts such as SHIEC members to ensure that all standards work effectively and can be implemented easily and economically.

Many industry barriers must be resolved for full adoption and utilization of any standardized and interoperable trusted exchange framework. Today, interoperability is significantly inhibited by variations across state and federal laws governing patient privacy. Unlike other industries where federal standards prevail in interstate commerce (e.g. banking, telecommunications, and aviation), HIPAA explicitly defers to any laws that are more protective of patient privacy whether federal (e.g.,

42 CFR Part 2), state or local. These complexities are well documented by the National Governor's Association in a recent 77-page publication (https://www.nga.org/files/live/sites/NGA/files/pdf/2016/1612HealthCareRightInformation.pdf.)

In addition, a trusted interoperable exchange framework must be economically viable for all participants. Many providers and health information exchange organizations have limited budgets and do not have an extensive number of funding sources to support costly technical infrastructure. Basic healthcare interoperability, with its dozens of required frameworks, taxonomies and administrative requirements, is a complex environment with many challenges and problems. Varying patient consent requirements significantly multiply complexities by requiring separate procedures based on each possible data source or destination. These variable consent requirements may result in healthcare providers using the "safest" business choice that keeps data in their home environment in order not to risk violation of another third party's process. This approach minimizes their exposure to potential risks such as lawsuits and the elimination of costly, unanticipated customizations.

The following, select examples present situations in which exchange capabilities are inhibited by today's environment with a result of preventing complete utilization of any interoperable exchange network.

Example 1 - Interstate data sharing: New York State has well-developed, patient consent laws regarding data exchange. HIEs and providers within the state have invested in infrastructure to comply with these laws. However, providers outside the state cannot easily obtain data from New York providers unless they invest in achieving compliance with New York laws. Providers in New Jersey and Pennsylvania may find value in making this investment, but providers and health information exchange organizations in other parts of the county may not be able to invest even though they may provide care for visiting New York residents.

Example 2—Interoperability with behavioral health: Behavioral health centers are medical homes to many of the most vulnerable, high-cost patients. For this segment of patients, interoperability could drive the greatest improvements in efficiency and quality. Many of these organizations are substance abuse treatment centers and design their systems to comply with 42 CFR Part 2. When their patients obtain care elsewhere, the patient data is effectively blocked, regardless of patient preference, simply because the combination of complexities both in administrative as well as technical designs that is required by the data source and the data recipient.

Example 3—HIPAA protections for individuals who request data withheld from health plans: Patients have the right to withhold health information from their health plans. Today, health plan and payer roles are evolving and requiring more patient information for business purposes. Likewise, providers are becoming accountable to health plans for the quality of care delivered and they can be financially penalized at times for protecting their patients' privacy when relevant episodes of care cannot be revealed due to certain circumstances. Organizations address this special exemption in different ways, ranging from withholding all data (since separating "self-pay" is considered administratively infeasible) to extensive and costly technical customizations and workflows. In all cases, the methods differ across organizations. This results in significant barriers, both technical and administrative that some might consider "information blocking," while others consider it essential for compliance.

We recommend that ONC consider the following action steps to work towards alleviating the barriers to information exchange that prohibit the full utilization of interoperable networks:

1. Support efforts to update HIPAA to take precedent in interstate commerce. Some argue that HIPAA does not protect privacy enough; however, when completely implemented and enforced, HIPAA sets a very high bar for patient privacy and holds providers to a high professional standard that address most concerns raised in support of privacy laws. We recognize there are many difficult policy issues to consider in this regard but believe that enabling interoperability is valuable enough to take on this effort.
2. Focus activities on aligning the numerous existing policies and regulations governing information exchange activities and those that impact exchange activities including HIPAA and 42CFR Part 2.
3. Encourage work to pass legislation to align all privacy rules such as the Overdose Prevention and Patient Safety Act, recently introduced in the House by Tim Murphy (R-PA) and Earl Blumenauer (D-OR).
4. Support efforts to revisit the self-pay provision in HIPAA, considering the underlying reasons for which the provision exists and provide new legislative recommendations to resolve current barriers. One example is found in the banking industry which depends on regulatory protections and insurance requirements to restore individuals' funds if they are victims of fraud, should the controls and protections intended to prevent fraud fail.

Comment Area 2: Transparency

A trusted exchange framework should conduct all exchange activities in an open and transparent manner. However, the effort to comply with state and federal regulations may inhibit the sharing of information and create the appearance of data blocking while, in some cases, even prevent the flow of data. Also limited transparency may occur from those engaged in information exchange. The key to a successful trusted exchange framework is TRUST. Many current "health information networks" are not widely trusted because the owners who control these networks can have conflicts of interest which are often undeclared. Many of these networks are governed by private interests or by public corporations who are motivated by financial interests in obtaining, storing, and reselling access to identified or de-identified data. Healthcare providers, who are entrusted with patients' private health information should not be required to "trust" health information networks that are not governed by individuals who represent the best interests of those who receive care, provide care, or pay for care in their community and region. As discussed in Comment Area 1 Standardization, ONC should develop a definition and requirements for a "trusted" health information network and framework. The requirements must include that the organization that owns and manages the network incorporates a governance body that is empowered to make decisions about all aspects of the handling of data in the network. The governance body should act as a neutral, non-commercial party representing the interests of those who provide, receive and pay for the care of the individuals that the network supports. The individuals should be appointed to this body through objective, well-established procedures that include protocols to publicly disclose and mitigate conflicts of interest with respect to the movement of health information and any financial interests.

Comment Area 3: Cooperation and Non-Discrimination

Any trusted exchange framework must provide mechanisms to support participants from freely sharing data. We encourage ONC to support the development of business use cases around the value of data sharing and best practices ensuring cooperation and non-discrimination. In addition, we also encourage ONC to provide opportunities for organizations to share their experiences and best practices. In doing this, ONC can lead the industry in determining "what" should be shared with whom while using specific use cases based on user needs, care setting and specific business requirements. Furthermore, patient health care data (PHI/PII) should not be considered a commodity used for financial gain. It should be shared freely to ensure patient information is available when it is needed unless specifically requested not to be shared by the patient. Discrimination in exchange among health information networks can often be attributed to the perception that other health information networks have conflicts of interest and will not act in the best interest of those whose information they are receiving. This is tightly associated with trust of the network within the community and participants. Trust is addressed in Comment Area 2 - Transparency.

We encourage ONC to work toward driving alignment across HIPAA and 42 CFR Part 2 which will not only facilitate data access and flow of patient information, but will serve to relieve industry confusion and the significant level of current, work effort required to comply with the various requirements.

The alignment of 42 CFR Part 2 would also alleviate significant barriers in achieving care delivery goals and support integration of the emerging participants in the care delivery ecosystem. Better alignment of regulations will encourage the expansion of exchange capabilities and alleviate fears associated with assumed risk and liability. Organizations who are Covered Entities under HIPAA, and their Business Associates, are accountable to the federal government for safeguarding the protected health information of patients. However, the health of individuals can often depend on the right decisions being made by people who are not HIPAA-covered entities, including health providers in free and charitable clinics, social service agencies (e.g., food banks, homeless shelters, religious communities, etc.) and municipal first responders. HIPAA provides well documented guidelines, and some current health information networks have found ways to appropriately incorporate non-covered entity health providers into appropriate data sharing arrangements. Many of these non-covered entities even agree to abide by HIPAA. However, these arrangements are not widespread since many covered entities perceive that disclosure, even for a HIPAA Permitted Purpose to any non-covered entity, creates a substantial risk that the covered entity will be held accountable under audit by federal enforcers for any breach by that non-covered entity even if that non-covered-entity has contractually pledged to comply with HIPAA and disclosures are made for permitted purposes under HIPAA.

Consideration should be given to the publication of additional guidance that specifically targets covered entities that are responsible for disclosing information for permitted purposes to non-covered entities. This approach would ensure confidence in successfully achieving HIPAA compliance with non-covered entities.

Comment Area 4: Security and Patient Safety

Any trusted exchange framework must be a secured environment that supports the patient's right to privacy with protection of their health information. This framework must ensure the highest degree of data integrity which can be supported through use of effective data and interoperability standards. It is critical that a trusted exchange framework ensure accurate patient identification and patient matching which will reduce medical errors and ensure high quality patient care and resulting clinical outcomes. While technology advances such as with mobile health and APIs are growing in availability, a trusted exchange framework must have mechanisms to accommodate new technology, standards and interoperability guidelines while ensuring data security. In addition, identification of best practices will ensure the most effective deployment and management of the exchange infrastructure ensuring data integrity. It is a balancing act to ensure patient safety and data security while providing access to clinical data at the point of care delivery regardless of location. The goal of any exchange framework is that data should reside in the most secure environment while liquid enough to be available when and where needed.

Comment Area 5: Access

A trusted exchange framework must be flexible and secure in providing access to information to the appropriate care provider at the point of care regardless of care location. In addition, a framework must accommodate patients, care givers and consumers who are demanding access to their information in a usable format for making informed health care decisions based on cost and quality.

Data silos remain even though significant progress has been made with exchange capabilities. The success of a trusted exchange framework is dependent on an environment that supports effective and economical use of standards, interoperability principles and data aggregation/analytics capabilities supporting data flow within and across regions and the nation. Use cases can be used to ensure that users have the most effective view or 'slice' of the data for their business uses. Today, some providers believe they have too much data while others believe they have too little data or that the data presentation is not useable, especially for clinical decision making. Intermediaries such as health information exchange organizations are serving as the community's trusted intermediary and providing the most effective access and presentation of the data to providers, patients and their families. SHIEC's Patient Centered Data Home ™ is one of the industry's trusted and secured exchange framework providing exchange and data access across regions and the nation.

Comment Area 6: Data – Driven Choice

A trusted exchange framework must have the capabilities to support data aggregation and analytics across many disparate sources with information presented in a consumable manner for all types of use cases and purposes ranging from patient care delivery and population management to consumer data needs such as evaluating health care services based on quality and cost. The success of a trusted exchange framework is dependent on having an environment that supports highly complex analysis and data views for many user types including providers, patients, consumers, payers, employers as well as other nontraditional data users. Mechanisms and incentives must be in place that promotes capabilities to achieve extensive data aggregation and analytics. While many vendors today provide aggregation capabilities at the provider level, the query response for clinical

information from multiple encounters and care givers may not be in a format that is easily reconciled at the provider level. Clinical and financial data may not be easily aggregated for analytic purposes at a population level. A trusted exchange framework must be a neutral platform providing access to data that can be used and consumed based on the end user business requirements.

General Comments

'No Safe Harbor' from conflicting interpretations of law:

Covered entities and business associates are liable for interpreting, implementing, and complying with HIPAA regulations. On policy matters, some covered entities have experienced inconsistency between guidance and enforcement by federal agencies. Expanding interoperability requires innovation and uncertainty, which risk-averse organizations, including many health systems, typically try to avoid. No organization wants to be the one discovered as the first example of "doing it wrong." We recommend that ONC provide a forum working with industry stakeholder where examples of compliance risks that cause covered entities to hesitate from participating in interoperability can be collected and discussed. This provides an opportunity for collaboration with all applicable federal sources to address the issues and publish resulting guidance from this effort. The published guidance should include all interpretations of the rule under which interoperability can occur and covered entities can assume trust for exchange that will be accepted as compliance with the regulation.

We would be glad to discuss these comments if you have questions or would like additional information. In addition, we offer the SHIEC volunteers as subject matter experts to work with ONC when moving forward with this important work. Thank you for your on-going commitment with the widespread adoption, implementation and use of interoperable systems and information exchange. We look forward to collaborating with ONC on this and other initiatives in the future.

Sincerely,

Charles E. Christian
Chair of the SHIEC Advocacy Committee
Vice President – Technology & Engagement
Indiana Health Information Exchange

Pam Matthews,
Interim Executive Director
Strategic Health Information Exchange Collaborative (SHIEC)