DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

45 CFR Part 171

Nationwide Health Information Network: Conditions for Trusted Exchange

AGENCY: Office of the National Coordinator for Health Information Technology (ONC), Department of Health and Human Services.

ACTION: Request for information.

SUMMARY: The nationwide health information network is defined as the set of standards, services, and policies that enable secure health information exchange over the Internet. Enacted in February 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act requires the National Coordinator for Health Information Technology to establish a governance mechanism for the nationwide health information network (section 3001(c)(8) of the Public Health Service Act (PHSA)). This request for information (RFI) is being issued to request public comment on draft proposals the Office of the National Coordinator for Health Information Technology (ONC) is considering in anticipation of developing a notice of proposed rulemaking (NPRM) to establish such a governance mechanism. This RFI seeks broad input on a range of topics, including: the creation of a voluntary program under which entities that facilitate electronic health information exchange could be validated with respect to their conformance to certain ONC-established "conditions for trusted exchange (CTEs);" the scope and requirements included in the initial CTEs; the processes that could be used to revise, adopt new, and retire CTEs, including but not limited to the standards development and adoption process provided in section 3004 and other relevant sections of the PHSA; and a process to

classify the readiness for nationwide adoption and use of technical standards and implementation specifications to support interoperability related CTEs.

DATES: To be assured consideration, written or electronic comments must be received at one of the addresses provided below, no later than 5 p.m. on [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may submit comments identified by any of the following methods below (please do not submit duplicate comments). Because of staff and resource limitations, we cannot accept comments by facsimile (FAX) transmission.

- Federal eRulemaking Portal: Follow the instructions for submitting comments. Attachments should be in Microsoft Word or Excel, Adobe PDF; however, we prefer Microsoft Word. http://www.regulations.gov.
- Regular, Express, or Overnight Mail: Department of Health and Human Services, Office of the National Coordinator for Health Information Technology, Attention: Governance RFI, Hubert H. Humphrey Building, Suite 729D, 200 Independence Ave, S.W., Washington, D.C. 20201. Please submit one original and two copies.
- Hand Delivery or Courier: Office of the National Coordinator for Health Information Technology, Attention: Governance RFI, Hubert H. Humphrey Building, Suite 729D, 200 Independence Ave, S.W., Washington, D.C. 20201. Please submit one original and two copies. (Because access to the interior of the Hubert H. Humphrey Building is not readily available to persons without federal government identification, commenters are encouraged to leave their comments in the mail drop slots located in the main lobby of the building.)

Inspection of Public Comments: All comments received before the close of the comment period will be available for public inspection, including any personally identifiable or confidential business information that is included in a comment. Please do not include anything in your comment submission that you do not wish to share with the general public. Such information includes, but is not limited to: a person's social security number; date of birth; driver's license number; state identification number or foreign country equivalent; passport number; financial account number; credit or debit card number; any personal health information; or any business information that could be considered to be proprietary. We will post all comments received before the close of the comment period at http://www.regulations.gov.

Docket: For access to the docket to read background documents or comments received, go to http://www.regulations.gov or the Department of Health and Human Services, Office of the National Coordinator for Health Information Technology, Hubert H. Humphrey Building, Suite 729D, 200 Independence Ave, S.W., Washington, D.C. 20201 (call ahead to the contact listed below to arrange for inspection).

FOR FURTHER INFORMATION CONTACT: Steven Posnack, Director, Federal Policy Division, Office of Policy and Planning, Office of the National Coordinator for Health Information Technology, 202-690-7151.

SUPPLEMENTARY INFORMATION:

Acronyms and Abbreviations

ACO	Accountable Care Organization
ARRA	American Recovery and Reinvestment Act
CDA	Clinical Document Architecture
CEHRT	Certified EHR Technology

CTEs	Conditions for Trusted Exchange
DURSA	Data Use and Reciprocal Support Agreement
EHR	Electronic Health Record
FIPPS	Fair Information Practice Principles
HIPAA	Health Insurance Portability and Accountability Act of 1996
HIT	Health Information Technology
HITECH	Health Information Technology for Economic and Clinical Health
IEC	International Electrotechnical Commission
IIHI	Individually Identifiable Health Information
ISO	International Organization for Standardization
NVEs	Nationwide Health Information Network Validated Entities
NCVHS	National Committee on Vital and Health Statistics
NPRM	Notice of Proposed Rulemaking
PHSA	Public Health Service Act
PHI	Protected Health Information
OCR	Office for Civil Rights
OIG	Office of the Inspector General
ONC	Office of the National Coordinator for Health Information Technology
RFI	Request for Information
RFP	Request for Proposal
RLS	Record Locator Services
S&I	Standards and Interoperability
S/MIME	Secure/Multipurpose Internet Mail Extensions

SMTP Simple Mail Transport Protocol

XDM Cross-Enterprise Document Media Interchange

XDR External Data Representation

Table of Contents

I. Background

A. Introduction

Electronic health information exchange (referred to as "electronic exchange" in the text that follows) addresses a critical need in our healthcare system and provides the foundation for improved care coordination and quality improvement. However, absent a common set of rules to guide its development and nationwide expansion, electronic exchange has been governed by a patchwork of contractual relationships, procurement requirements, State and Federal laws, and industry self-regulation through accreditation and certification. Consequently, this ad-hoc governance approach has led to asymmetries in the policies and technical standards, which are evident in the various local, regional and State electronic exchange activities. Because of the expected increase in demand for electronic exchange capacity to support innovative care and payment models now underway as well as proposed meaningful use Stage 2 objectives and measures, stakeholders have communicated to the Office of the National Coordinator for Health Information Technology (ONC) that a consistent, baseline set of "rules of the road" for electronic exchange is desirable, and perhaps necessary.

We believe that this is an opportune time to solicit input on how the governance mechanism for the nationwide health information network should be shaped and how we could effectively use our statutory authority to complement existing Federal regulations to support and enable nationwide electronic exchange. We also believe that a properly crafted governance mechanism could yield substantial public benefits, including: reduced burden and costs to engage in electronic exchange; added protections for consumers and health care providers; and, in the long-run, a more innovative, and efficient electronic exchange marketplace that would ultimately create an environment where electronic exchange is commonplace and "worry-free."

For individual consumers, one of the governance mechanism's potential benefits could be the establishment of additional safeguards specific to electronic exchange that are not addressed by other Federal laws, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules, or State laws. For example, the governance mechanism could include more prescriptive and/or more stringent policies for entities that facilitate electronic exchange than are included in the HIPAA Privacy and Security Rules. From a health care provider's perspective, we anticipate that the governance mechanism could provide assurances to all electronic exchange parties that a specified set of requirements have been met. In turn, we believe these assurances could help spur greater trust and confidence in electronic exchange among providers and ease concerns associated with sharing patient information. Finally, for the entities that facilitate electronic exchange, we believe that the governance mechanism could enable a more competitive and open electronic exchange market and make it more efficient for these entities to exchange electronic health information.

B. Governance Mechanism Overview

This request for information (RFI) reflects ONC's current thinking regarding the approach ONC should take to establish a governance mechanism for the nationwide health information network. It frames many of the draft proposals and concepts ONC is considering, and depending on comments ONC receives, many of these concepts could be included in a future notice of proposed rulemaking. We seek public comment on whether it is timely for ONC to act to establish a governance mechanism; the advantages, disadvantages, and anticipated market impact of the potential proposals we discuss; and whether we should consider any alternatives in place of, or in combination with, the proposals discussed in this RFI.

Overall, we believe that it would be impracticable and imprudent to establish through regulation a "one-size fits all" approach to governance. Given the constantly evolving technical and policy landscape applicable to electronic exchange, it would be onerous and perhaps unachievable to specify up front all forms of electronic exchange to which the governance mechanism could apply. Rather, we view the nationwide health information network as a continually expanding ecosystem of electronic exchange activities for which stakeholders would be able to select the appropriate set of standards, services, and policies to meet their electronic exchange needs. This ecosystem would encompass many forms of electronic exchange, ranging from simple forms (such as when the electronic exchange of health information is planned and sent to a known destination) to more sophisticated forms (such as when the electronic exchange is unplanned meaning the data source is unknown beforehand and query and response techniques are utilized). It would also accommodate emerging exchange activities as they gain policy and technical maturity, such as the use cases being proven by the participants in the nationwide health information network Exchange initiative[1]. Thus, just as the nationwide health information network is defined by the evolving set of standards, services, and policies of which it is comprised, so too, we believe, should its governance mechanism.

In rulemaking, we would seek to launch the structures, processes, and initial requirements that would be necessary for the governance mechanism to operate. In subsequent rulemakings, we anticipate addressing evolving electronic exchange requirements and the standards and policies necessary to effectively govern new and perhaps more complex forms of electronic exchange. Below, we briefly summarize the proposals this RFI covers and provide more detailed explanations for each proposal in the sections that follow.

[1] Additional information on the Exchange can be found on ONC's website at: http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__nhin_exchange/1407

- Adoption of "conditions for trusted exchange" (CTEs). CTEs would reflect the nationwide health information network's portfolio of standards, services, and policies and would be incrementally added to and refined over time. The initial set of CTEs included in this RFI conceptually represent many of the CTEs that we believe are foundational for enabling trusted nationwide electronic exchange to occur, regardless of the form of electronic exchange in which one engages. CTEs would be established under three categories: interoperability; safeguards; and business practices. We believe that CTEs generally would constitute "standards" and "implementation specifications" as described in the HITECH Act for purposes of conducting electronic exchange under the auspices of the nationwide health information network.
- Establishment of a voluntary framework for entities that facilitate electronic exchange to be validated to CTEs adopted for the electronic exchange services or activities they are capable of supporting. This framework would be similar to the health information technology (HIT) certification programs ONC has already established via regulation (76 FR 1262)[2], but would focus on the services and activities the entities perform in facilitating electronic exchange and not exclusively on HIT itself. Upon successful validation to adopted CTEs an entity would be recognized as a nationwide health information exchange network validated entity (NVE) and thus become responsible for performing electronic exchange services in accordance with the adopted CTEs.
- Approaches for monitoring and transparent oversight. Such approaches would seek to ensure the integrity of the governance mechanism by protecting consumer rights, instilling industry-wide confidence in the services performed by NVEs, and provide a

[2] Information on ONC's Permanent Certification Program for HIT can be found on ONC's website at: http://origin.www.gpo.gov/fdsys/pkg/FR-2011-01-07/pdf/2010-33174.pdf

way to receive and address complaints as well as a process to revoke an NVE's validation status.

- Establishment of processes that could be used to adopt, revise, and retire CTEs that are no longer appropriate. This would entail developing a CTE maturity lifecycle process to identify, modify, and retire CTEs over time.
- Establishment of a process to classify the readiness for nationwide adoption and use of technical standards and implementation specifications to support interoperability related CTEs. Due to their rapidly evolving nature, we believe an annual review process to assess and classify the maturity and adoptability of technical standards and implementation specifications would be beneficial.

We have intentionally presented many details of our considerations in this RFI. We hope that this level of detail will generate more specific and insightful comments and a more comprehensive dialogue. In establishing a governance mechanism, ONC is committed to obtaining ongoing public input, and we are consequently also relying heavily on the HIT Policy Committee[3] and HIT Standards Committee recommendations related to governance of the nationwide health information network.[4] Our overall objectives for establishing a governance mechanism for the nationwide health information network are, among others, to improve the efficiency of electronic exchange among providers, reduce provider implementation costs (such as the cost of interfaces), and assure the privacy and security of the data being exchanged. Furthermore, we anticipate that an entity's validation to the CTEs could be leveraged by others to accomplish other policy and programmatic objectives. For example, Federal programs that

[3] Additional information on the HIT Policy and Standards Committees can be found on the ONC website at: http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__federal_advisory_committees_%28facas%29/1149

[4] The HIT Policy Committee and HIT Standards Committee were established in law by the HITECH Act and advise and issue recommendations to the National Coordinator on issues concerning HIT policy and standards.

participate in electronic exchange could require the use of entities that are validated in accordance with the CTEs adopted as part of the nationwide health information network governance mechanism.

C. Historical Context

1. Statutory Authority.

The Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA) (Pub. L. 111–5), was enacted on February 17, 2009. The HITECH Act amended the Public Health Service Act (PHSA) and established "Title XXX—Health Information Technology and Quality" to improve health care quality, safety, and efficiency through the promotion of HIT and the electronic exchange of health information. More specifically, section 3001(c)(8) of the PHSA, requires the National Coordinator for Health Information Technology (National Coordinator) to "establish a governance mechanism for the nationwide health information network." Thus we interpret section 3001(c)(8) of the PHSA with sufficient breadth to enable the National Coordinator to establish a mechanism for governing the nationwide health information network, which we define as the set of standards, services, and policies that enable secure health information exchange over the Internet.[5]

We note that Congress in section 3001(b) of the PHSA directed the National Coordinator to perform his duties under section 3001(c) in a manner "consistent with the development of a nationwide health information technology infrastructure that allows for the electronic use and exchange of information" and that accomplishes the eleven outcomes specified in PHSA section 3001(b) for which the National Coordinator is responsible. Moreover, we believe the authority

[5] Overview information of the nationwide health information network can be viewed on ONC's website at: http://healthit.hhs.gov/portal/server.pt?open=512&objID=1142&parentname=CommunityPage&parentid=4&mode=2

granted to the National Coordinator at section 3001(c)(1)(A) to "review and determine whether to endorse each standard, implementation specification, and certification criterion for the electronic exchange and use of health information that is recommended by the HIT Standards Committee under section 3003 for purposes of adoption [by the Secretary] under section 3004" as well as the National Coordinator's authority to consider policy recommendations from the HIT Policy Committee as described in section 3002(b) of the PHSA would support the approach we are considering to establish for the nationwide health information network governance mechanism.

Section 3002(b)(2)(A) of the PHSA authorizes the HIT Policy Committee to "recommend the areas in which standards, implementation specifications and certification criteria are needed for the electronic exchange and use of health information for purposes of adoption under section 3004 and [to] recommend an order of priority for the development, harmonization, and recognition of standards, specifications, and certification criteria…." Section 3002(b)(3) states "[t]he HIT Policy Committee shall serve as a forum for broad stakeholder input with specific expertise in policies relating to the matters described in paragraphs (1) and (2)."

Section 3003(b)(1)(A) of the PHSA states that "[t]he HIT Standards Committee shall recommend to the National Coordinator standards, implementation specifications, and certification criteria described in subsection (a) that have been developed, harmonized, or recognized by the HIT Standards Committee. . .." Section 3003(b)(2) directs the HIT Standards Committee to "serve as a forum for the participation of a broad range of stakeholders to provide input on the development, harmonization, and recognition of standards, implementation specifications, and certification criteria necessary for the development and adoption of a

nationwide health information technology infrastructure that allows for the electronic use and exchange of health information."

Lastly, section 3004 of the PHSA in turn identifies a process for the adoption of HIT standards, implementation specifications, and certification criteria and authorizes the Secretary to adopt such standards, implementation specifications, and certification criteria.

2. Overview of Select Existing Federal Health Information Privacy and Security Standards

The success of electronic exchange under the auspices of the nationwide health information network depends, in large part, on assurances that personally identifiable health information will remain confidential and secure. Existing Federal standards governing the privacy and security of health information establish an essential baseline of protection on which we anticipate building through nationwide health information network governance.

The Privacy and Security Rules issued under HIPAA established the first generally applicable Federal protections for health information maintained by certain key segments of the health care industry: health care providers who transmit health information electronically in connection with a transaction for which the Secretary has adopted a standard, health plans, and health care clearinghouses (collectively called "covered entities"). The HIPAA Privacy Rule sets the standards and implementation specifications for the use and disclosure of individually identifiable health information (IIHI) held by these covered entities (called protected health information or PHI). It is notable that the HIPAA Privacy Rule was not intended to establish best practices with which covered entities could voluntarily comply; rather, it establishes a

baseline of enforceable Federal regulatory protections upon which the States or covered entities (as a matter of organizational policy) are free to expand.[6]

The HIPAA Security Rule requires covered entities to establish specific administrative, physical, and technical safeguards[7] for electronic protected health information (as such term is defined at 45 CFR 160.103). The HIPAA Security Rule is scalable and flexible to account for the varying size, resources, technology and security risks faced by covered entities as they protect the electronic health information for which they are responsible.[8] The HIPAA Security Rule includes both standards and implementation specifications, which provide instructions for implementing certain of the standards. The implementation specifications set out in the Security Rule fall into two categories: those that are "required" and those that are "addressable." An entity must implement a "required" implementation specification. In contrast, an entity has some flexibility in implementing an "addressable" implementation specification based on a variety of factors, such as, among others, the entity's risk analysis, risk mitigation strategy, what security measures are already in place, and the cost of implementation.[9] Encryption, for example, is an addressable implementation specification.

Subtitle D of the HITECH Act (sections 13400 – 13424) expanded the protections afforded by HIPAA by requiring, among other things, business associates (generally, persons or entities that create, receive, maintain, or transmit PHI on behalf of, or in the provision of certain

[6] (2000) The HIPAA Privacy Final Rule, published at 65 Fed. Reg. 82462 at 82471.
[7] (2010) The regulatory references to administrative, physical, and technical safeguards can be found, respectively, at Part 164, Sections 308, 310, and 312 of Title 45 of the CFR.
[8] More information on the HIPAA Security Rule can be found on the Office for Civil Rights website at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html
[9] An addressable implementation specification requires an assessment to determine whether implementation would be reasonable and appropriate safeguard in the particular entity's environment. Following the assessment, the entity must implement the specification if it finds it to be reasonable and appropriate. If the outcome of the assessment is that implementing the specification would not be reasonable and appropriate, then the entity must (1) document why it would not be reasonable and appropriate to implement the specification; and (2) implement an equivalent alternative measure if reasonable and appropriate.

services to, a covered entity) to comply with certain HIPAA Privacy Rule provisions and the standards and implementation specifications of the Security Rule.

3. Health Information Exchange and the Nationwide Health Information Network in Brief

Over the past decade the nationwide health information network has been conceptualized in several different ways. The following provides a brief history of the major activities, events, and milestones that have shaped our understanding and conceptualization of the nationwide health information network.

a. 2001-2004: Conceptualization and Request for Information

In 2001, the National Committee on Vital and Health Statistics (NCVHS) issued recommendations on nationwide electronic health information exchange within a report titled "Information for Health, A Strategy for Building the National Health Information Infrastructure." In this report, NCVHS outlined three dimensions of health information infrastructure (Personal Health; Healthcare Provider; and Population Health) that would be important for "conceptualizing the capture, storage, communication, processing, and presentation of information." NCVHS also recognized that ensuring the confidentiality and security of personal health information was paramount in developing the infrastructure to enable nationwide electronic health information exchange. Noting that the HIPAA Privacy Rule provided strong protections for individually identifiable health information, the NCVHS also forecasted that additional protections would be needed to extend across all the users, technologies, and functions envisioned by the nationwide health information network.

Since 2004, when the Office of the National Coordinator for Health Information Technology (ONC) was created under Executive Order 13335, ONC has supported the

development of standards, services, and policies to support nationwide electronic exchange. ONC's first formal step was the publication of a request for information in November 2004 which sought public input on the development of the nationwide health information network which was originally characterized as a "network of networks." ONC received 512 comments in response to the RFI and published a report summarizing the comments the following year.[10] Comments addressed a number of issues such as governance, financing, and how the nationwide health information network could be coordinated along with local and regional health information exchange projects. With respect to governance, comments indicated that "a well-built governance model was needed to develop, set policies and standards for, operate, and promote the adoption of a nationwide health information network" and discussed the merits of governance options that ranged from significant Federal involvement to a State government-sponsored approach to an approach that involved public-private collaboration.

b. 2005-2008: Nationwide Health Information Network Exchange – Prototypes and Trial Implementations

In June 2005, ONC took another step forward toward the development of the nationwide health information network when it issued a request for proposals (RFP) for the development of nationwide health information network prototype architectures. The prototypes sought to test a range of services including the capabilities to query and retrieve health information from health information exchange organizations; the delivery of new data to appropriate recipients; patient identification and matching; information locator services; and user

[10] (2005) ONC. "Summary of Nationwide Health Information Network (NHIN) Request for Information (RFI) Responses." Available at: http://www.hhs.gov/healthit/rfisummaryreport.pdf

authentication, access control and other security protections.[11] The prototypes also explored the feasibility and scalability of potential nationwide health information network models. In fall 2005, ONC awarded four organizations contracts based on the RFP.[12]

In October 2006, NCVHS issued recommendations to ONC on a minimum, but critical, set of functional requirements for nationwide electronic health information exchange to take place. These recommendations sought to accommodate diverse architectures across networks and systems[13] and followed a report issued by NCVHS earlier in the year regarding privacy and confidentiality considerations for the nationwide health information network.[14]

In fall 2007 and spring 2008, building on the experiences gained and lessons learned in the prototype phase, ONC awarded contracts and grants to organizations to conduct nationwide health information network trial implementations.[15] Among these organizations' accomplishments in the context of the trial implementations was the development of data and interface specifications, testing materials, and a draft model data use and reciprocal support agreement (DURSA).[16] The DURSA, a single, multi-party agreement, specified the rules of engagement and obligations to which all participants in the trial implementations agreed to adhere. It also underscored a framework for broad-based information exchange among a set of trusted entities, reflecting consensus (among the signatories) on policies such as: privacy and

[11] More information on the prototype architectures can be viewed on ONC's website at: http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__nhin_historical___background_information/1409

[12] (2005) The archived announcement can be viewed on the HHS website at: http://archive.hhs.gov/news/press/2005pres/20051110.html

[13] (2006) The NCVHS recommendations can be viewed on the NCVHS website at: http://www.ncvhs.hhs.gov/061030lt.pdf

[14] (2006) "Privacy and Confidentiality in the Nationwide Health Information Network." NCVHS, available at: http://www.ncvhs.hhs.gov/060622lt.htm

[15] (2007) The announcement can be viewed on the HHS website at: http://www.hhs.gov/news/press/2007pres/10/pr20071005a.html

[16] Additional information on the DURSA can be viewed on the S&I Framework website at: http://jira.siframework.org/wiki/display/OBTI/DURSA+Overview

security obligations; duties of requesting and responding participants; responding participants' legal requirements; and the allocation of liability risk.

Also during this time, NCVHS published informative reports with recommendations related to how entities engaged in electronic exchange activities but who are not covered by HIPAA should be treated and the policy issues associated with consent and secondary uses of IIHI.[17,18,19]

The prototype and trial implementation phases produced important insights. Most significantly, they identified areas where further technical and policy work would be needed to enable query and retrieve-based electronic health information exchange and they highlighted the potential limitations of a single, multi-party data use agreement. As a result of these insights, ONC shifted its approach from a singular vision focused on the establishment of a network of networks to one in which the Federal government could serve as the facilitator of diverse approaches to electronic exchange through the specification of nationally-accepted standards, services, and policies. This transition was based in part on the recognition that there could be multiple types of electronic exchange networks all built on the same foundational building blocks of standards, services, and policies.

c. 2009-Present: Nationwide Health Information Network Production and Governance

Beginning in 2009, Federal and non-Federal entities participating in the trial implementations began securely exchanging health information bound by the parameters

[17] (2007) NCVHS. "Update to privacy laws and regulations required to accommodate NHIN data sharing practices." Available at: http://ncvhs.hhs.gov/070621lt2.pdf
[18] (2007) NCVHS. "Enhanced Protections for Uses of Health Data: A Stewardship Framework for 'Secondary Uses' of Electronically Collected and Transmitted Health Data." Available at: http://ncvhs.hhs.gov/071221lt.pdf
[19] (2008) NCVHS. "Individual control of sensitive health information accessible via the Nationwide Health Information Network.." Available at: http://ncvhs.hhs.gov/080220lt.pdf

established in a "production DURSA." This confederation of entities is referred to as the "Nationwide Health Information Network Exchange" or "the Exchange," and relies on the DURSA to help structure a governance framework. To become a participant in the Exchange, an organization must sign the DURSA and also must pass an "onboarding"[20] test to demonstrate capacity to meet the DURSA's technical interoperability requirements.

Presently, a growing number of organizations are exchanging health information as part of the Exchange. Participants in the Exchange are engaged in production activities that include: the exchange of summary patient records for care coordination, including health information that is part of the Virtual Lifetime Electronic Record and which is jointly sponsored by the Departments of Defense and Veterans Affairs; the exchange of summary patient records for Social Security Administration disability determination purposes; and biosurveillance and case reporting to the Centers for Disease Control and Prevention. These use cases have helped to define and evolve a set of specific standards, services, and policies included in the nationwide health information network's growing electronic exchange portfolio.

Many lessons can be learned from the Exchange's production activities. For instance, the Exchange identified one type of governance model for nationwide electronic health information exchange with the DURSA, which relies upon a "Coordinating Committee" and "Technical Committee," to develop exchange policies and technical interoperability requirements for the participants. Another important lesson learned was that the member organizations identified a need for more specific policies and greater consistency in implementing the HIPAA Privacy and Security Rules in order to engender sufficient trust among parties with which data would be shared. The Exchange's efforts have aided in the early identification and resolution of policy

[20] More information regarding onboarding procedures can be viewed on the S&I Framework website at: http://jira.siframework.org/wiki/display/OBTI/Home

and technical challenges and helped tee up issues that require broad stakeholder dialogue, such as the policy and technical requirements related to matching patients to their health information.

d. Private Sector Electronic Exchange

Payment and delivery reforms – from accountable care organizations (ACOs)[21] to bundled payments and medical homes – are creating a compelling business case for electronic exchange. As a result, innovative approaches to electronic exchange are emerging, including private networks advanced by hospital systems pursuing ACO status, exchange services offered by electronic health record (EHR) vendors, and regional and state-level health information exchange initiatives. According to a recent KLAS survey, the number of active private health information exchange entities tripled from 52 in 2009 to 161 in 2010.[22]

e. The Direct Project

Stage 1 of the Medicare and Medicaid EHR Incentive Programs included several objectives and measures that required or encouraged electronic exchange as an efficient means for an eligible professional, eligible hospital, or critical access hospital to satisfy the objective and measure (e.g., "exchange key clinical information;" "incorporate clinical lab test results;" and "submission to immunization registries"). As we reviewed our standards portfolio in terms of its ability to support meaningful use Stage 1, we determined that we were missing a simple and easily adoptable approach to enable electronic exchange to occur. While many HIT vendors supported some kind of planned electronic exchange capability prior to meaningful use Stage 1, many did not follow a common set of standards or included a proprietary mechanism that would make it difficult for providers using different systems to easily exchange clinical information to support patient care.

[21] More information on accountable care organizations can be viewed on the CMS website at: https://www.cms.gov/ACO/

[22] (2011) KLAS Research. "Health Information Exchanges: Rapid Growth in an Evolving Market."

In March 2010, after public meetings held by the HIT Policy Committee, ONC coordinated the launch of the "Direct Project" to identify the standards, services, and policies necessary to enable a simple, secure, scalable, standards-based way for participants to send authenticated, encrypted health information directly to known, trusted recipients over the Internet. The Direct Project focused on what would be necessary to transport health information regardless of the clinical content of the information to be exchanged. A primary goal of the Direct Project was to support secure, efficient, and low cost exchange of health information and to make it possible for eligible health care providers to satisfy some of the meaningful use Stage 1 objectives and associated measures that require electronic exchange.

Unlike the Exchange, the Direct Project cannot rely on a governance framework provided by the DURSA and "onboarding" procedures. While both initiatives are considered part of ONC's nationwide health information network activities, each was established to address different electronic exchange requirements and contribute different standards, services, and policies to the nationwide health information network's portfolio. A basic analogy that may help explain the relationship between the nationwide health information network, the Exchange, and the Direct Project is as follows: the nationwide health information network is akin to the "Internet" – an electronic environment in which the use of a common set of standards, services, and policies will allow a group of entities to exchange information. The nationwide health information network comprises multiple approaches that one could use to electronically exchange electronic health information among a variety of stakeholders. The Exchange could be compared to a consortium using a secure "Intranet," in which only approved members can gain access after receiving the appropriate security credentials and agreeing to the Intranet's terms of use. Continuing this analogy, the Direct Project is like secure email or even secure instant

messaging, whereby two entities that already share a trust relationship with each other can use relatively simple technical means to electronically exchange health information.

f. The Health Information Technology Policy and Standards Committees' Work on the Nationwide Health Information Network.

In September 2010, the HIT Policy Committee, which is one of two statutorily established Federal Advisory Committees that provide advice to the National Coordinator, formed the nationwide health information network Governance Workgroup (Governance Workgroup) and charged it with "draft[ing] a set of recommendations on the scope and process of governance for nationwide health information exchange, including measures to ensure accountability and oversight."[23] When developing its recommendations for the HIT Policy Committee, the Governance Workgroup held a series of public meetings and received testimony from diverse stakeholders.[24] After receiving the Governance Workgroup's recommendations, the HIT Policy Committee deliberated on them, concurred with them, and formally transmitted them to the National Coordinator for consideration in December 2010.[25] The following bullets summarize the recommendations to the National Coordinator. The recommendations:

- Identified nine core principles according to which the nationwide health information network should be governed. These principles included: transparency and openness; inclusive participation and adequate representation; effectiveness and efficiency; accountability; federated governance and devolution; clarity of mission and consistency

[23] The complete list of Governance Workgroup members can be viewed on the ONC website at: http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&objID=3080

[24] As background, ONC also provided prior NCVHS reports and a 2009 whitepaper developed by the National eHealth Collaborative which framed certain governance functions.

[25] The complete set of recommendations can be viewed on the ONC website at: 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_letter_gov_wg_dec2010.pdf

of actions; fairness and due process; promote and support innovation; and finally, evaluation, learning and continuous improvement.

- Emphasized that the nationwide health information network should be considered a preferred approach for nationwide health information exchange.
- Identified the responsibilities for the Federal government in governance of the nationwide health information network. These should include: 1) Leading the development of fundamental "conditions" to facilitate greater trust and interoperability in an electronic health information exchange environment and promote the adoption of those conditions through various policy levers; 2) Recognizing existing state authorities across all relevant domains and facilitating coordination and harmonization with states and other entities as needed; 3) Requiring exchange with Federal agencies to be conditioned on compliance with the conditions; and 4) Sharing the responsibility of governance with other entities to reflect a "governance of governances."
- Optimize broad stakeholder input, including consumers, to facilitate the conditions needed for greater trust and interoperability in electronic exchange.
- Establish an initial set of conditions and a process to incrementally add to or modify the conditions over time. Establish a process to validate[26] the adopted conditions accounting for the cost and burden, and to leverage existing validation methods, processes, and entities where appropriate.
- Ensure accountability through oversight.

[26] The HIT Policy Committee noted that the term "validation" was used to generally refer to the process of verifying compliance and may include a broad array of possible methods (e.g., self-attestation, testing, certification of systems, accreditation of entities). In our use of the term validation throughout this document, we mean it to encompass both accreditation and certification.

Most recently, the HIT Standards Committee established a subcommittee, the nationwide health information network Power Team, in June 2011.[27] The Power Team was charged with: 1) creating a draft set of criteria for evaluating standards, including factors such as adoptability and scalability: 2) evaluating the specifications developed for the Exchange and Direct Project initiatives with respect to their ability to support nationwide health information exchange; and 3) recommending those specifications that could be integrated and deployed to support the secure transport and exchange of electronic health information on a national scale, and identifying where further work may be needed. The Power Team held a series of public meetings and drafted a set of recommendations[28] for the HIT Standards Committee, noting that while neither the Exchange nor the Direct Project's specifications have been proven at scale, there was minimal risk in adopting transport mechanisms based on the Direct Project specifications. They also recommended simplifying existing specifications for the Exchange and investing in pilots for representational state transfer (REST) or "RESTful" approaches to electronic exchange. On September 28, 2011, the HIT Standards Committee transmitted a letter to the National Coordinator reflecting the analysis conducted by the Power Team.

II. Request for Information

A. Establishing a Governance Mechanism

As we consider how best to implement our statutory authority to establish a governance mechanism for the nationwide health information network, we believe it would be critical to adopt a suite of conditions for trusted exchange (CTEs) to serve as the "rules of the road" for trusted, secure, and interoperable electronic exchange, nationwide. We believe that the CTEs

[27] The complete list of Workgroup members can be viewed on the ONC website at: http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&objID=3850

[28] The complete set of recommendations can be viewed on the ONC website at: http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__standards_recommendations/1818

could serve as a foundational set of requirements that could be used in one or more combinations to support many different forms of electronic exchange. CTEs appear to best be grouped into three categories: safeguards, interoperability, and business practices.

- Safeguards CTEs would focus on the protection of IIHI to promote its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure.
- Interoperability CTEs would focus on the technical standards for the exchange and integration of electronic health information so that it is useful for the recipient.
- Business Practices CTEs would focus on the operational and financial practices or standards to which NVEs would need to adhere in support of trusted electronic exchange.

Question 1: Would these categories comprehensively reflect the types of CTEs needed to govern the nationwide health information network? If not, what other categories should we consider?

An important component of the governance mechanism we are considering would be the establishment of a voluntary framework for entities that facilitate electronic exchange to be validated to CTEs adopted for the exchange services or activities they are capable of supporting. Upon successful validation to the CTEs, an entity would be recognized as a NVE and thus would be recognized as an entity that would be accountable for the electronic exchange services or activities it performs in accordance with the CTEs. Given the incremental CTE adoption approach we expect to take, we also anticipate that the recognition of NVEs would incrementally expand along with the diversity of the electronic exchange services or activities they are able to perform. Thus, we could see providing NVEs or new entities with other categorical

recognition(s) for the electronic exchange services or activities they are capable of supporting in accordance with subsequently adopted CTEs. Additionally, this validation process would support an evolution, in the U.S. and internationally, towards engaging accountability agents as a supplemental means for ensuring that organizations and providers involved in the management, storage, and transport of IIHI adhere to policies and practices that protect the privacy and security of information.

It is also our expectation that validation would be voluntary. In other words, the validation process established as part of the governance mechanism would not be mandatory and would only apply in so far as an entity deciding that there would be value (e.g., prestige, competitive advantage) in seeking validation. That said, once the validation process is established, much like other government programs on which subsequent policy objectives could be leveraged, it would be possible for other public and private organizations to specify NVE recognition as a condition in awarding contracts, procurements and/or in other situations where validation would be beneficial.

Question 2: What kind of governance approach would best produce a trusted, secure, and interoperable electronic exchange nationwide?

Question 3: How urgent is the need for a nationwide governance approach for electronic health information exchange? Conversely, please indicate if you believe that it is untimely for a nationwide approach to be developed and why.

Question 4: Would a voluntary validation approach as described above sufficiently achieve this goal? If not, why?

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

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

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

B. Actors and Associated Responsibilities

We intend to use notice and comment rulemaking to establish the structures, processes, and initial requirements that would be necessary for the governance mechanism to operate. Under the governance mechanism we are considering, ONC would retain certain responsibilities to ensure the governance mechanism's proper implementation, but would also seek to delegate, where possible and appropriate, certain other responsibilities that we believe can best be performed by the private sector.

1. ONC

Generally speaking, we anticipate that the National Coordinator's and ONC's responsibilities as part of the governance mechanism would include:

- Endorsing and adopting CTEs, in accordance with the National Coordinator's authority at section 3001(c)(1)(A) and processes identified at section 3004 under the PHSA, and publishing interpretative guidance on the means to comply with adopted CTEs;

- Facilitating the receipt of input from the HIT Policy and Standards Committees and other interested parties on revisions to CTEs, new CTEs, and the appropriate retirement of CTEs in accordance with processes identified at sections 3002(b)(3) and 3003(b)(2) of the PHSA;
- The selection and oversight processes for an accreditation body that would be responsible for accrediting organizations interested in becoming validation bodies;
- Authorizing and overseeing validation bodies which would be responsible for validating that eligible entities have met adopted CTEs;
- Administering a process to classify the readiness for nationwide adoption and use of technical standards and implementation specifications to support interoperability related CTEs; and
- Overall oversight of all entities and processes established as part of the governance mechanism.

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

2. The Accreditation Body and Validation Bodies

Similar to the roles and responsibilities we established under the permanent certification program for HIT (76 FR 1262), we could see establishing a process by which the National Coordinator would approve a single body to accredit and oversee "validation bodies." The process considered in this RFI, however, would differ from the HIT certification programs in that validation would evaluate an entity's conformance to adopted CTEs as opposed to a particular product's (e.g., EHR technology) certification to certification criteria. We could envision,

however, certified HIT (in other venues referred to as commercial off-the-shelf software) being used by an entity as a way to demonstrate conformance with certain adopted CTEs. For this to occur, we anticipate that we would have to adopt specific certification criteria that could be used to subsequently certify other types of HIT through our already established HIT certification program. The accreditation body would be expected to conform to internationally accepted standards for accreditation bodies, and in particular, the standard ISO/IEC 17011: 2004, jointly published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), which specifies requirements for assessing and accrediting certification bodies. The validation bodies (upon accreditation by the accreditation body and authorization from the National Coordinator) would subsequently perform the validation of entities' conformance to adopted CTEs. Ultimately, we believe that validation could encompass many different methodologies (e.g., self-attestation; laboratory testing for standards conformance; certification; and accreditation) and could vary depending on the type of CTE and the potential burden the validation methodology would impose.

Question 9: Would a voluntary validation process be effective for ensuring that entities engaged in facilitating electronic exchange continue to comply with adopted CTEs? If not, what other validation processes could be leveraged for validating conformance with adopted CTEs? If you identify existing processes, please explain the focus of each and its scope.

Question 10: Should the validation method vary by CTE? Which methods would be most effective for ensuring compliance with the CTEs? (Before answering this question it may be useful to first review the CTEs we are considering to adopt, see section "VI. Conditions for Trusted Exchange.")

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?

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?

3. Entities Eligible for Validation

a. Eligible Entities

We anticipate that potential NVEs could include, but would not be limited to, the following types of entities that provide services to facilitate electronic health information exchange: EHR developers; regional, state, local or specialty-based health information exchanges; health information service providers; State agencies; Federal agencies, and integrated delivery networks.

b. Eligibility Criteria

In order to provide a baseline level of trust in NVEs, we think that it could be helpful to establish upfront eligibility criteria such as the ones discussed below. We are considering that entities interested in becoming NVEs would need to:

- Meet all solvency and financial responsibility requirements imposed by the statutes and regulatory authorities of the State or States in which it, or any subcontractor performing some or all of its functions, would serve. We are considering requiring a prospective NVE make some type of financial disclosure filing as well as provide evidence that it has a surety bond or some other form of financial security.

- Have the overall resources and experience to fulfill its responsibilities in accordance with the CTEs when performing health information exchange services. We are considering whether an entity would need to have at least one year of experience.
- Serve a sufficient number of providers to permit a finding of effective and efficient administration. Under this criterion, however, no prospective NVE would be deemed ineligible if it only served providers located in a single State.
- Have to be a valid business or governmental entity operating in the United States.
- Have not 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.
- Not be listed on the Excluded Parties List System maintained by the General Services Administration which includes information regarding entities debarred, suspended, proposed for debarment, excluded or disqualified under the non-procurement common rule, or otherwise declared ineligible from receiving Federal contracts, certain subcontracts, and certain Federal assistance and benefits.
- Not be listed on the List of Excluded Individuals and Entities maintained by the Office of Inspector General (OIG). The OIG has the authority to exclude individuals and entities from Federally funded health care programs pursuant to sections 1128 and 1156 of the Social Security Act and maintains a list of all currently excluded individuals and entities called the List of Excluded Individuals and Entities.

We include the HIPAA civil money penalty criterion as we expect that most entities that would qualify as NVEs would be business associates of covered entities as defined in the HIPAA Rules, or in some cases covered entities themselves, and therefore, would be directly subject to

the requirements and standards of the HIPAA Privacy, Security and Breach Notification Rules. Additionally, we do not believe that it would be appropriate to have an eligibility criterion that limits eligible entities to only those that are tax-exempt under section 501(c)(3) of the Internal Revenue Code (IRC). Finally, in the case of Federal or State governmental entities seeking to become an NVE, we anticipate that some of the eligibility criteria we are considering may be inapplicable.

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

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?

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

Question 16: Should eligibility be limited to entities that are tax-exempt under section 501(c)(3) of the IRC? If yes, please explain why.

4. Stakeholders

Throughout the history of the nationwide health information network, a strong emphasis has been placed on ensuring broad stakeholder participation in the network's development and governance.

Question 17: What is the optimum role for stakeholders, including consumers, in governance of the nationwide health information network? What mechanisms would most effectively implement that role?

C. Monitoring and Transparent Oversight

As the HIT Policy Committee and stakeholder feedback over time have indicated, any governance mechanism established for the nationwide health information network would need to include some method for monitoring and transparent oversight. To mitigate confusion in the marketplace, protect consumer rights, and help ensure health care provider satisfaction, we believe a process to receive and address complaints as well as a process to revoke an NVE's status would need to exist. While the revocation of an NVE's status may be the most severe "penalty" ONC could impose, we also realize that when a penalty is so substantial there can be a tendency to pursue other measures to correct an identified issue except in the case of severe violations.

We also anticipate that monitoring and transparent oversight could be conducted by different stakeholders as part of nationwide health information network governance. While ONC could retain overall authority for monitoring and oversight, we also believe that the accreditation body and validation bodies involved in determining compliance with the adopted CTEs could also play oversight roles. For example, validation bodies would be responsible for monitoring and overseeing the NVEs they have validated. Furthermore, other modes of monitoring and enforcement could also play a role, such as: voluntary industry self-policing, a complaint/ombudsman role for a non-governmental entity, civil lawsuits. That said, we do not believe that some of these enforcement or monitoring methods would necessarily be effective, particularly in light of the voluntary validation framework we are considering. Moreover, Federal agencies including the Federal Trade Commission (FTC) and the HHS Office for Civil Rights (OCR) have enforcement authority within their regulatory jurisdictions and can already act on complaints of certain improper conduct. For instance, the FTC could investigate alleged misconduct related to validation status through the Federal Trade Commission Act (15 U.S.C. §§

45(a) and 52). A negative determination could lead to revoking an NVE's public representation of conformance to the adopted CTEs. Similarly, OCR, which enforces the HIPAA Privacy and Security Rules, could investigate alleged violations of the HIPAA Rules, the outcome of which could impact an NVE's validation of conformance to certain CTEs.

Question 18: What are the most appropriate monitoring and oversight methods to include as part of the governance mechanism for the nationwide health information network? Why?

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

If we were to pursue a validation approach, we believe that entities that have been successfully validated in accordance with the CTEs should be able to publicly represent themselves in some manner as complying with the adopted CTEs. We think this public representation could stimulate market demand for NVE services in the health information exchange marketplace.

We assume that NVEs would need to conform to some CTEs regardless of the specific electronic health information exchange service(s) or activities provided. We believe this approach could create a core trust baseline for all NVEs and that such commonality could strengthen the public's trust of NVEs and NVEs' trust of other NVEs. Finally, we assume that some NVEs could perform services or activities unrelated to adopted CTEs. In such cases, we believe it would be necessary for there to be a clear distinction between the recognition an NVE receives under the governance mechanism and the other services or activities it supports but for which validation has not been provided.

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?

Question 21: How long should validation status be effective?

D. Conditions for Trusted Exchange (CTEs)

We recognize and expect that electronic health information exchange capacity will continue to accelerate over the coming years. With this additional capacity, new ways for individuals to fully participate in their health care, and activities to harness this capacity to improve population health and develop a "learning health care system" will be available. As we closely watch other activities in the public and private sectors, we anticipate that the CTEs we are considering in this first rulemaking will need to be revised, that other CTEs will need to be retired to reflect the changing electronic health information exchange landscape, and that new CTEs will be needed. Our goal in discussing this initial set of CTEs is to identify a starting point, and then eventually support as broad a range of electronic exchange activities as practicable given the maturity of technical standards and policies for electronic exchange. The following discussion reflects ONC's current thinking regarding a first set of CTEs that could be adopted to support a variety of electronic exchange activities, nationwide.

1. Safeguards CTEs

A Code of Fair Information Practice was first articulated by an Advisory Committee to the Secretary of the US Department of Health, Education, and Welfare in a 1973 report, *Records, Computers, and the Rights of Citizens.* The Code is well accepted as a foundation for protecting

the privacy of individually identifiable information, and many privacy laws are based on it, both in the United States and abroad. The principles that underlie the Code also served in part as the bases on which HHS developed its 2008 Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information (Privacy and Security Framework).[29] The Privacy and Security Framework includes eight principles that are expected to guide the actions of all persons and entities that participate in a network for the purpose of electronic exchange of IIHI. Wherever applicable, we have endeavored to represent these principles within the Safeguard CTEs we discuss. We have also attempted to reflect principles underlying the HIT Policy Committee recommendations in the relevant CTEs.

We assume that most NVEs will perform services involving the use or disclosure of IIHI on behalf of health plans and health care providers. Accordingly, we believe that nearly all NVEs would be HIPAA business associates of health plans and health care providers and, pursuant to the HITECH Act, subject to the use and disclosure standards and implementation specifications of the HIPAA Privacy Rule as well as the security standards and implementation specifications in the HIPAA Security Rule. We expect these NVEs would comply with these rules.

Although the HIPAA Privacy and Security Rules would apply to nearly all NVEs in some way, the governance mechanism and specifically the CTEs would, in part, serve to address limited instances of electronic exchange not covered under the privacy and security protections afforded by the HIPAA Privacy and Security Rules. First, the CTEs would extend privacy and security requirements to non-HIPAA-covered entities and non-HIPAA-business associates that engage in nationwide electronic exchange. Second, the CTEs would establish additional

[29] (2008) ONC. "Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information." Available at: http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__privacy___security_framework/1173

requirements not currently addressed by the HIPAA Privacy and Security Rules. Finally, the HIPAA Privacy Rule sets required baseline protections and was not necessarily intended to reflect best practices[30] and the HIPAA Security Rule is scalable and flexible to account for the varying size, resources, technology and security risks faced by covered entities.[31] However, given the nature of the services NVEs will be performing, we believe that it would be appropriate and justified in the context of electronic exchange for NVEs to be held to a more uniform set of practices and policies than those that may be adopted to comply with the HIPAA Privacy and Security Rules.

- **Condition [S-1]:** An NVE must comply with sections 164.308, 164.310, 164.312, and 164.316 of title 45 of the Code of Federal Regulations as if it were a covered entity, and must treat all implementation specifications included within sections 164.308, 164.310, and 164.312 as "required."

For most health care organizations in the United States, the HIPAA Security Rule is the preeminent framework for securing electronic health information. Published in February 2003, the HIPAA Security Rule sets forth a flexible and scalable approach to apply to a broad range of HIPAA covered entities, including covered provider practices (large and small), payers, and health care clearinghouses, all of which have different needs and resources with respect to securing electronic health information in their environments. In providing this flexibility, the HIPAA Security Rule provides both "required" and "addressable" implementation specifications. Covered entities must meet the "required" implementation specifications, but are

[30] (2000). Final Rule. 65 Fed. Reg. 82462 at 82471. Available at: http://www.gpo.gov/fdsys/pkg/FR-2000-12-28/pdf/FR-2000-12-28.pdf
[31] (2003). Final Rule. 68 Fed. Reg. at 8335. Available at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf

permitted to take equivalent, alternative approaches to "addressable" implementation specifications if the covered entity has determined that such implementation specifications would not be reasonable or appropriate for the entity's particular environment. In 2009, with the enactment of the HITECH Act, Congress specified that sections 164.308, 164.310, 164.312, and 164.316 of title 45 of the Code of Federal Regulations shall apply to business associates in the same manner as they apply to covered entities. Accordingly, and because we believe that nearly all NVEs will be business associates of covered entities (or covered entities themselves), we believe that mirroring this statutory requirement is the best starting point for NVEs' overall security practices. That being said, one of our main goals in establishing a governance mechanism for the nationwide health information network is to establish a consistent trust baseline for electronic exchange. Thus, we believe that in order to strengthen the public's trust of NVEs and NVEs' trust of other NVEs that all of the HIPAA Security Rule's "addressable" implementation specifications should be required for all NVEs. We believe that this approach provides greater certainty and more uniformity with respect to the security practices NVEs would need to follow.

Question 22: Are there HIPAA Security Rule implementation specifications that should not be required of entities that facilitate electronic exchange? If so, which ones and why?

Question 23: Are there other security frameworks or guidance that we should consider for this CTE? Should we look to leverage NISTIR 7497 Security Architecture Design Process for Health Information Exchanges[32]? If so, please also include information on how this framework would be validated.

[32](2010) NIST. "Security Architecture Design Process for Health Information Exchanges (HIEs)." Available at: http://csrc.nist.gov/publications/nistir/ir7497/nistir-7497.pdf

- **Condition [S-2]:** An NVE must only facilitate electronic health information exchange for parties it has authenticated and authorized, either directly or indirectly.

We believe that it is important for an NVE to offer the parties for which it facilitates exchange a high degree of certainty that only authorized parties are able to use its exchange services. The requirement to authenticate and authorize the parties for which the NVE facilitates exchange could be accomplished either directly or indirectly by the NVE. In the case of the latter, the NVE would need to require the party for which it facilitates electronic exchange to perform authentication and authorization in order to be in compliance with this CTE. We believe that if an NVE cannot directly authenticate and authorize the parties for which it facilitates exchange (which could be at an organizational level), that it would be critical for the NVE to "flow down" these responsibilities and obtain reasonable assurance from the party(ies) for which it facilitates exchange that only authenticated and authorized personnel are able to access electronic exchange services it facilitates. For example, if the NVE were to facilitate an electronic exchange for a hospital, it would be able to satisfy this CTE (indirectly) by ensuring that the hospital had a process in place to authenticate and authorize its own personnel's use of the exchange services provided by the NVE. In proposing the adoption of this CTE, we would also look to NIST SP800-63(v1.02) "Electronic Authentication Guideline" and any other best practices available to determine the appropriate authentication requirements NVEs would need to satisfy in facilitating electronic exchange.

Question 24: What is the most appropriate level of assurance that an NVE should look to achieve in directly authenticating and authorizing a party for which it facilitates electronic exchange?

Question 25: Would an indirect approach to satisfy this CTE reduce the potential trust that an NVE could provide? More specifically, should we consider proposing specific requirements that would need to be met in order for indirect authentication and authorization processes to be implemented consistently across NVEs?

Question 26: With respect to this CTE as well as others (particularly the Safeguards CTEs), should we consider applying the "flow down" concept in more cases? That is, should we impose requirements on NVEs to enforce upon the parties for which they facilitate electronic exchange, to ensure greater consistency and/or compliance with the requirements specified in some CTEs?

- **Condition [S-3]:** An NVE must ensure that individuals are provided with a meaningful choice regarding whether their IIHI may be exchanged by the NVE.

In considering the recommendations that we received from the HIT Policy Committee[33], we believe that individuals should be able to exercise meaningful choice with respect to how their electronic health information is exchanged. The HIT Policy Committee explained that "meaningful choice" could be either an opt-in or opt-out model[34], or more granular consents so long as individuals or their legal designees are adequately and clearly informed about how and why their information will be exchanged, in advance of making a decision whether to participate in electronic exchange. The HIT Policy Committee also stated that the process of providing meaningful choice should include communicating to an individual the following: 1) that choice is not a condition of receiving medical treatment; 2) that the choice will be commensurate with

[33](2010). The complete set of recommendations can be viewed on the ONC website at: 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

[34] In an opt- out model, by default, all or some predefined set of data is automatically eligible for exchange, with a provision that patients must be given the opportunity to request that their data not be eligible for exchange. In contrast, in an opt-in model, by default, no patient data is automatically eligible for exchange. Patients wishing to make all, or a pre-defined set, of their information available must actively express their desire to make their data eligible for exchange.

the circumstances for why IIHI is being exchanged; 3) that the choice is consistent with reasonable patient privacy, health, and safety expectations; and 4) that the choice is revocable – that is it can be retracted.

In terms of providing meaningful choice, we believe that an NVE should be required to do the following to satisfy this CTE, either: directly provide the patient with meaningful choice regarding the exchange of their IIHI; or ensure (with some means of verification) that the health care provider for which it facilitates electronic exchange has provided individuals with meaningful choice regarding the exchange of their IIHI.

Mindful that the HIT Policy Committee's recommendations are premised on the belief that different means of exchange may invoke different privacy and security concerns, we are considering, within the context of Interoperability CTE I-1[35], what exceptions to the provision of meaningful choice would be prudent. We are considering the following three situational exceptions within this specific context: 1) when the NVE is engaging in the exchange of IIHI for purposes of medical treatment; 2) when information exchange is mandatorily required under law; or 3) the NVE is acting solely as a conduit and not accessing or using IIHI beyond what is required to encrypt and route it to its intended destination. For example, if we were to adopt a CTE that excluded those purposes it would mean that no patient choice would be required when one provider purposefully elects to electronically exchange health information directly with another provider for treatment purposes (e.g., sending a referral to a specific provider, transmitting a prescription) beyond what is required in current law or what has been customary practice. The HIT Policy Committee has yet to assess and provide recommendations to the National Coordinator on the circumstances under which meaningful choice should be required

[35] An NVE must be able to facilitate secure electronic health information exchange in two circumstances: 1) when the sender and receiver are known; and 2) when the exchange occurs at the patient's direction.

for other electronic exchange purposes. We note, however, that the HIPAA Privacy Rule sets a baseline that requires express authorization (an opt-in approach) for certain purposes, such as marketing with very limited exceptions.

Question 27: In accommodating various meaningful choice approaches (e.g., opt-in, opt-out, or some combination of the two), what would be the operational challenges for each approach? What types of criteria could we use for validating meaningful choice under each approach? Considering some States have already established certain "choice" policies, how could we ensure consistency in implementing this CTE?

Question 28: Under what circumstances and in what manner should individual choice be required for other electronic exchange purposes?

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 following Interoperability CTE I-1?

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?

- **Condition[S-4]:** An NVE must only exchange encrypted IIHI.

Encryption is often regarded as a best practice for maintaining the confidentiality of IIHI transmitted across networks. To satisfy this condition, we believe that an NVE would need to be able to either 1) exchange already encrypted IIHI, 2) encrypt IIHI before exchanging it, or 3) establish and make available encrypted channels through which electronic exchange could take place (or do any combination of the above). We would expect NVEs to implement industry best

practices for doing so. In order to provide some degree of flexibility, we would establish a general CTE for encryption of data in motion and publish more specific guidance on best practices. These requirements and guidelines would be consistent with the guidance provided by HHS' OCR related to breach notification and standards for rendering unsecured protected health information unusable, unreadable, or indecipherable to unauthorized individuals.[36]

Question 31: Should there be exceptions to this CTE? If so, please describe these exceptions.

- **Condition [S-5]:** An NVE must 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.

Under the HIPAA Privacy Rule (45 CFR 164.520), individuals have the right to adequate notice of the uses and disclosures of their protected health information, a right which a covered entity fulfills by furnishing a notice of privacy practices (NPP). Generally speaking, the HIPAA Privacy Rule NPP must include a description of the types of uses and disclosures a HIPAA covered entity is permitted to make for treatment, payment, and health care operations, as well as a description of other uses and disclosures which are permitted without the individuals' written authorization.

The type of notice contemplated by this CTE would differ in certain aspects from a HIPAA Privacy Rule NPP. First, rather than a notice directed only to consumers whose health information is being used or disclosed, we believe that NVEs should clearly give advance notice to those who use their services, as well as to the general public, why they collect IIHI, how it is used, and to whom and for what reason it is disclosed. Second, with the goal of increasing

[36] (2009). Interim Final Rule. 74 Fed Reg at 42740. Available at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html

public trust and enabling electronic exchange, we believe that an NVE should give notice about what it actually does do, rather than what it is legally permitted to do, with the IIHI for which it is responsible for exchanging. Third, we believe a NVE should give explicit and specific notice about certain uses and disclosures of health information, such as the specific circumstances when it will de-identify health information and provide it to third parties. For example, if the NVE de-identifies IIHI and then provides such de-identified information to pharmaceutical or research companies, it would need to include a description of this action in its notice to satisfy the CTE described above. This would address the concerns of some stakeholders, including certain members of the HIT Policy Committee, that certain persons and organizations may not be fully aware that an entity transmitting data on their behalf may de-identify their data and then share such de-identified data with third parties. We also believe this CTE is consistent with the privacy and security "core values" recommended by the HIT Policy Committee on September 1, 2010.

Question 32: Are there specific uses or actions about which we should consider explicitly requiring an NVE to be transparent?

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

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

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

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?

- **Condition [S-6]:** An NVE must not use or disclose de-identified health information to which it has access for any commercial purpose.

As noted above, some stakeholders, as well as the HIT Policy Committee, have expressed concern that certain persons may not be fully aware that someone transmitting data on their behalf may use de-identified data for profit seeking opportunities. This scenario appears to have raised two concerns: the potential that certain recipients of de-identified data possess their own established databanks and may be able to re-identify the data by comparing it to existing data; and providers' losing trust in a system in which the data for which they are responsible, although de-identified, is monetized. We recognize that under the HIPAA Privacy Rule, a provider could prohibit a business associate in its business associate agreement from de-identifying data and then subsequently using the de-identified data. However, we are aware of circumstances where certain business associates have drafted business associate agreements that allow for such de-identification of data for the business associates' purposes. Additionally, smaller covered entities may lack the economic resources and expertise necessary to effectively negotiate business associate agreements, in particular with respect to preventing the commercialization of health information. We believe that having a CTE prohibiting NVEs from using or disclosing de-identified health information for economic gain would alleviate the concerns that have been

raised about potential re-identification of the data.[37] We also believe that such a prohibition would increase providers' trust in exchanging their data through an NVE.

Question 37: 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?

Question 38: On what other entities would this have an effect?

- **Condition [S-7]:** An NVE must operate its services with high availability.

We are considering requiring NVEs to demonstrate that the systems and processes they have in place can assure users that its services will be available when needed. We consider high availability to mean near 24 hours a day, 7 days a week availability. In other words, to demonstrate compliance with this CTE, an NVE would need to ensure its services would be available at all times, except for very limited, scheduled periods of time. We believe such a requirement is necessary because the need to engage in electronic exchange may occur at any time. In cases where two or more NVEs are necessary to route health information from the source to its ultimate destination, NVEs should have reasonable assurances that the other parties on which they depend to route health information will be available for electronic exchange.

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

- **Condition [S-8]:** If an NVE assembles or aggregates health information that results in a unique set of IIHI, then it must provide individuals with electronic access to their unique set of IIHI.

The HIPAA Privacy regulations at 45 CFR 164.524 provide individuals with a right to access information maintained in a Designated Record Set (as defined at 45 CFR 164.501).

[37] We believe that the risks for re-identification are somewhat exaggerated, but recognize that public concerns about this issue may undermine trust and impede the development of the standards, services, and policies that define the nationwide health information network.

However, this right may not extend to all IIHI that is used or assembled by NVEs to facilitate electronic exchange. Consistent with the "Access" principle expressed in the Privacy and Security Framework, we are considering adopting a CTE that would require an NVE to provide individuals with access to any information the NVE creates that results in a unique set of IIHI. In this context, and for the purpose of this CTE, we consider the IIHI that an NVE assembles or aggregates itself and retains on an individual to constitute a "unique set of IIHI" because the NVE would be the only party through which this information could be accessed (i.e., the individual would not be able to readily recreate the NVE's unique set of IIHI by requesting access to the information held by each of his or her providers that have a relationship with the NVE). For example, if multiple health care providers seek to electronically exchange health information for a given patient, then the NVE facilitating these exchanges would be in a position to aggregate the patient data it receives thus generating a unique set of IIHI. This CTE would require that an individual have access to this unique set of IIHI if he or she is unable to access the same set of information through some other singular channel (e.g., by making a standard HIPAA access request to a single health care provider).

Question 40: What further parameters, if any, should be placed on what constitutes a "unique set of IIHI"?

- **Condition [S-9]:** If an NVE assembles or aggregates health information which results in a unique set of IIHI, then it must provide individuals with the right to request a correction and/or annotation to this unique set of IIHI.

Building on the Safeguard CTE [S-8] above and consistent with the "Correction" principle in the Privacy and Security Framework, we believe that any NVE that must provide an individual with the right to access the unique set(s) of IIHI it maintains, should also be required

to provide individuals with the right to request a correction and/or annotation to this unique set of IIHI.

Question 41: If an NVE were to honor an individual's request for a correction to the unique set of IIHI that it maintains, what impact could such a correction have if the corrected information was accessible by health care providers and not used solely for the NVE's own business processes?

Question 42: Are there any circumstances where an NVE should not be required to provide individuals with the ability to correct their IIHI?

- **Condition [S-10]:** An NVE must have the means to verify 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.

The HIPAA Privacy Rule does not set specific requirements for when a health care provider may request information maintained by other providers for treatment purposes. The duty to protect health information is placed almost exclusively on the discloser, and the requester bears little responsibility.[38] More specifically, the HIPAA Privacy Rule permits providers to request and disclose information about a patient "to carry out treatment" without qualifying that the information must be for the treatment of that particular patient. This means that providers who may participate in health information exchange through an NVE based on the query and response model are permitted by HIPAA to disclose an individual's information for treatment purposes, and to have the NVE make the disclosure on their behalf, even if the recipient is treating a patient that is not the subject of the record.

[38] A covered entity requesting protected health information from another covered entity must adhere to the minimum necessary standard with respect to what information is requested; however, disclosures to or requests by a health care provider for treatment purposes are not subject to these minimum necessary restrictions. 45 C.F.R. 164.502(b).

In theory, a query and response model would allow a provider to seek records of unknown individuals by querying on a particular diagnosis or demographic information and retrieve all records responsive to the query.[39] If the provider had any treatment purpose for such a query, even if she lacked an actual treatment relationship with each patient whose record she received, there would not be a violation of the HIPAA Privacy Rule. We believe that in order to ensure trust in the query and response model, that: 1) as a business practice, the NVE should restrict access to patient data for treatment purposes to providers who have or are in the process of establishing a treatment relationship with the patient; and 2) that as a safeguard CTE, the NVE be required to have mechanisms in place to verify that such a relationship exists.

Question 43: What method or methods would be least burdensome but still appropriate for verifying a treatment relationship?

Question 44: Are there circumstances where a provider should be allowed access through the NVE to the health information of one or more individuals with whom it does **not** have a treatment relationship for the purpose of treating one of its patients?

2. Interoperability CTEs

As previously described, Interoperability CTEs would focus on the technical conditions for electronic exchange. This would include the standards and implementation specifications needed to ensure that electronic health information can be exchanged in a manner that allows for consistent and meaningful interpretation across systems. While this initial set of Interoperability CTEs primarily focuses on transport standards and conditions needed to support planned electronic exchange, we believe that they could also include, where appropriate or necessary for

[39] The President's Council of Advisors on Science and Technology report, *Realizing the Full Potential of Health Information Technology to Improve Healthcare for Americans: The Path Forward*, (Dec. 2010), for example, proposes a Google-like search engine for health information that would facilitate such queries.

electronic exchange to take place, additional specificity in the form of content exchange standards and vocabulary/code set standards.

Condition [I-1]: An NVE must be able to facilitate secure electronic health information exchange in two circumstances: 1) when the sender and receiver are known; and 2) when the exchange occurs at the patient's direction.

This Interoperability CTE would address "planned" electronic exchange scenarios when the sender and receiver are known (e.g., public health reporting, transitions of care) and scenarios when the exchange occurs at the patient's direction or with the patient's knowledge. An NVE seeking validation to facilitate planned electronic exchange would need to be able to do so according to secure specifications. We anticipate that this first governance rulemaking would focus solely on the specifications NVEs would need to be able to use to transport electronic health information for planned electronic exchange and would not focus on content exchange or vocabulary standards which we have largely addressed through our regulations related to EHR technology certification.

To satisfy this CTE, we are considering requiring an NVE to implement and use one of two types of transport specifications. The first type includes the transport specifications developed under the Direct Project, which are the Applicability Statement for Secure Health Transport, and the Cross-Enterprise Document Reliable Interchange (XDR) and Cross-Enterprise Document Media Interchange (XDM) for Direct Messaging. The second type includes the transport specification developed under the Exchange, SOAP-Based Secure Transport RTM version 1.0.[40,41]

[40] The specification document can be viewed on The Direct Project website at: http://wiki.directproject.org/Documentation+Library

[41] The specification document can be viewed on the S&I Framework website at: http://modularspecs.siframework.org/NwHIN+SOAP+Based+Secure+Transport+Artifacts

The Applicability Statement for Secure Health Transport specification describes how electronic health information can be securely transported using simple mail transport protocol (SMTP), Secure/Multipurpose Internet Mail Extensions (S/MIME), and X.509 certificates. The XDR and XDM for Direct Messaging specification describes the use of XDR and XDM as a means to transport electronic health information and would serve as a bridge between entities using/following web services and SMTP transport methods. We believe these two options would make it possible for a majority, if not all, interested entities who facilitate planned electronic exchange to satisfy this CTE.

Question 45: What types of transport methods/standards should NVEs be able to support? Should they support both types of transport methods/standards (i.e., SMTP and SOAP), or should they only have to meet one of the two as well as have a way to translate (e.g., XDR/XDM)?

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?

- **Condition [I-2]:** An NVE must follow required standards for establishing and discovering digital certificates.

Digital certificates are used to create a high-level assurance that an organization exchanging electronic health information is the entity it claims to be. Therefore, having common baseline expectations for establishing digital certificates and making the public keys discoverable are foundational elements for rapid, scalable electronic exchange. In this regard, in April 2011, the HIT Standards Committee approved and transmitted a set of recommendations on digital certificates for the National Coordinator to consider. Digital certificates are used both as part of

the transport specifications developed under the Direct Project as well as the Exchange to authenticate entities involved in electronic exchange. For the purposes of this CTE, we are considering adopting as requirements the recommendations expressed by the HIT Standards Committee, specifically its recommendations on the requirements and evaluation criteria for digital certificates. We are also considering its second recommendation with respect to cross-certifying with the Federal Bridge Certificate Authority (the Federal Bridge).

Question 47: Are the technical specifications (i.e., Domain Name System (DNS) and the Lightweight Directory Access Protocol (LDAP)) appropriate and sufficient for enabling easy location of organizational certificates? Are there other specifications that we should also 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[42]?

- **Condition [I-3]:** An NVE must 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.

The intent of this CTE is to provide guidance for NVEs to verify and match message subjects (i.e., patients) using a record locater services, master patient index, or another approach. In February 2011, the Privacy and Security Tiger team issued a set of recommendations to the HIT Policy Committee regarding patient matching. The recommendations centered on standardizing demographic data fields, evaluating matching consistency, accountability, developing and disseminating best practices, and supporting the role of the individual patient.

[42] Additional information on the Federal Bridge can be viewed at: http://www.idmanagement.gov/pages.cfm/page/Federal-PKI

Subsequently, the HIT Standards Committee formed the Patient Matching Power Team to further explore these recommendations. The Patient Matching Power Team focused specifically on the use case of near time, direct patient care.[43]

Before exploring the specifications for patient matching, the Power Team first developed a set of baseline assumptions around the appropriate levels of specificity and sensitivity. For this use case, the Power Team assumed that specificity was more critical than sensitivity and that specificity of at least 99.9% and sensitivity of 95% would be an appropriate range for ensuring a high level of matching accuracy and accountability. These levels were used because sensitivities lower than 95% could result in incomplete views of the patient's record and specificities lower than 99.9% could result in incorrect matching, putting both the patient and the inappropriately matched individual at risk.

In August 2011, the Patient Matching Power Team presented several recommendations relating to patient matching to the HIT Standards Committee, which were considered, adopted and submitted to the National Coordinator. Its recommendations included a general principle regarding matching sensitivity and specificity and suggested that a base set of patient attributes should be selected based on demonstrated achievement of those levels. The HIT Standards Committee also recommended that health care providers give patients more of a role in verifying attributes used for matching and that HIT developers should provide a method for identifying missing or unavailable data to be identified and further, that basic validity checks be performed on patient attributes (such as only accepting dates in the past for dates of birth, no more than six 9s or six 0s in a row in the Social Security Number). Finally, the HIT Standards Committee recommended that patient query patterns should follow the "Exchange patient query

[43] The complete set of recommendations can be viewed on the ONC website at: http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__standards_recommendations/1818

implementation guide" and that the CDA R2 header formats should be used to represent patient attributes. It was also noted that responses to patient queries should not return any patient attributes that were not included in the original query, but that it may be appropriate for the response to indicate other data that could be useful in matching this patient.

Question 49: Should we adopt a CTE that requires NVEs to employ matching algorithms that meet a specific accuracy level or a CTE that limits false positives to certain minimum ratio? What should the required levels be?

Question 50: What core data elements should be included for patient matching queries?

Question 51: What standards should we consider for patient matching queries?

3. Business Practice CTEs

The third category of CTEs we are considering would focus on an NVE's business practices, including the operational and financial practices to which an NVE would need to adhere. We believe this category of CTEs would be necessary in order to ensure electronic exchange among NVEs takes place unimpeded.

- **Condition [BP-1]:** An NVE must send and receive any planned electronic exchange message from another NVE without imposing financial preconditions on any other NVE.

Generally speaking, this CTE expresses our belief that any health care provider using an NVE should be able to engage in unimpeded, planned electronic health information exchange with another health care provider using a different NVE. We believe that requiring NVEs to meet this CTE would instill greater confidence in planned electronic health information exchange and among health care providers who would rely on NVEs. In satisfying this CTE, an NVE could not impose business requirements on other NVEs, such as fees that would otherwise prevent another NVE from exchanging electronic health information on behalf of its customer

(e.g., a doctor). We believe this CTE would be especially relevant in preventing instances where an NVE with a significant share of the market would try to leverage their market dominance to impose an economic "rent" on other NVEs (e.g., excessive fees), resulting in market distortions. It would also prevent an NVE from making it difficult for their customers – those using the services offered by the NVE – to conduct electronic exchange with another NVE.

Question 52: Should this CTE be limited to only preventing one NVE from imposing a financial precondition on another NVE (such as fees), or should it be broader to cover other instances in which an NVE could create an inequitable electronic exchange environment?

Question 53: 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?

Question 54: Under what circumstances, if any, should an NVE be permitted to impose requirements on other NVEs?

- **Condition [BP-2]:** An NVE must provide open access to the directory services it provides to enable planned electronic exchange.

In order for planned electronic exchange to take place, and to satisfy this CTE, NVEs would need to make openly available to other NVEs or NVE customers certain services they offer. For example, for electronic exchange to take place following the Direct Project specifications, it would be necessary for an NVE to make openly available a directory of addresses of potential recipients and locatable public keys. While we recognize that the industry is still building its capacity to address this CTE, we believe that it is achievable.

- **Condition [BP-3]:** An NVE must report on users and transaction volume for validated services.

In order to assess our progress towards nationwide availability and use of health information exchange, it would be useful to have data about the use of NVE services, the types of users, and transaction volume for their validated services. The data should be collected and made available at the aggregate level so as not to expose information about specific customers or patients.

Question 55: What data would be most useful to be collected? How should it be made available to the public? Should NVEs be required to report on the transaction volume by end user type (e.g., provider, lab, public health, patient, etc)?

E. Request for Additional CTEs

Stakeholders are encouraged to provide feedback on this initial set of CTEs and in submitting comments suggest other CTEs that we should also consider. The following table summarizes the CTEs as presented in this RFI.

CTE Category	CTE
Safeguards	[S-1]: An NVE must comply with sections 164.308, 164.310, 164.312, and 164.316 of title 45 of the Code of Federal Regulations as if it were a covered entity, and must treat all implementation specifications included within sections 164.308, 164.310, and 164.312 as "required."
Safeguards	[S-2]: An NVE must only facilitate electronic health information exchange for parties it has authenticated and authorized, either directly or indirectly.
Safeguards	[S-3]: An NVE must ensure that individuals are provided with a meaningful choice regarding whether their IIHI may be exchanged by the NVE.
Safeguards	[S-4]: An NVE must only exchange encrypted IIHI.
Safeguards	[S-5]: An NVE must 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.
Safeguards	[S-6]: An NVE must not use or disclose de-identified health information to which it has access for any commercial purpose.
Safeguards	[S-7]: An NVE must operate its services with high availability.
Safeguards	[S-8]: If an NVE assembles or aggregates health information that results in a unique set of IIHI, then it must provide individuals with electronic access to

	their unique set of IIHI.
Safeguards	[S-9]: If an NVE assembles or aggregates health information which results in a unique set of IIHI, then it must provide individuals with the right to request a correction and/or annotation to this unique set of IIHI.
Safeguards	[S-10]: An NVE must have the means to verify 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.
Interoperability	[I-1]: An NVE must be able to facilitate secure electronic health information exchange in two circumstances: 1) when the sender and receiver are known; and 2) when the exchange occurs at the patient's direction.
Interoperability	[I-2]: An NVE must follow required standards for establishing and discovering digital certificates.
Interoperability	[I-3]: An NVE must 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.
Business Practices	[BP-1]: An NVE must send and receive any planned electronic exchange message from another NVE without imposing financial preconditions on any other NVE.
Business Practices	[BP-2]: An NVE must provide open access to the directory services it provides to enable planned electronic exchange.
Business Practices	[BP-3]: An NVE must report on users and transaction volume for validated services.

One approach for implementing nationwide electronic exchange can be observed through the Nationwide Health Information Network Exchange. As we described in the background section of this RFI, the Exchange is a confederation of trusted entities that have passed certain requirements for participation. One such requirement includes signing the DURSA, which serves as a legal framework for sharing electronic health information among participants in the Exchange. The DURSA includes "performance and service specifications" which the participating members agree to use in implementing secure electronic exchange. The most recent specifications used by participants in the Exchange can be found on ONC's website.[44] These specifications focus on a range of different electronic exchange activities, including specifications for: "Patient Discovery;" "Query for Documents;" "Retrieve Documents;"

[44] The Exchange specifications can be viewed on the ONC website at: http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__nhin_resources/1194

"Authorization Framework;" "Web Services Registry;" "Access Consent Policies;" and other such specifications with a yet to be determined effective date.

Question 56: Which CTEs would you revise or delete and why? Are there other CTEs not listed here that we should also consider?

Question 57: Should one or more of the performance and service specifications implemented by the participants in the Exchange be included in our proposed set of CTEs? If so, please indicate which one(s) and provide your reasons for including them in one or more CTEs. If not, please indicate which one(s) and your reasons (including any technical or policy challenges you believe exist) for not including them in one or more CTEs.

Question 58: In the notice of proposed rulemaking (NPRM) we intend to subsequently issue, should the above CTEs as well as any others we consider for the NPRM be packaged together for the purposes of validation? In other words, would it make sense to allow for validation to different bundles of safeguard, interoperability, and business practice CTEs for different electronic exchange circumstances?

Question 59: Should we consider including safe harbors for certain CTEs? If so, which CTEs and what should the safe harbor(s) be?

F. CTE Processes and Standards and Implementation Specification Classifications

1. CTE Life Cycle

Assuming we were to pursue an approach that includes the adoption of CTEs as part of a governance mechanism for the nationwide health information network, we expect that additional CTEs and revisions to CTEs would be necessary to accommodate policy maturity and technical changes over time. We believe that an inclusive and transparent process to identify, modify, and

retire CTEs would be needed to engage stakeholders and would result in more refined and widely accepted CTEs. The purpose of this process would be to identify and assess current electronic exchange needs and to provide a path for determining how best to address them through the CTEs. We envision that rulemaking could be necessary every two years, most likely on years that would alternate with regulations published for EHR Incentive Programs, to keep the CTEs up-to-date and to permit entities to seek validation to new CTEs for other more complex forms of electronic exchange.

We believe that an approach to a CTE maturity life cycle could start with the identification of "emerging" CTEs, followed by the identification of "pilot" CTEs, followed by "national" candidate CTEs which we would consider sufficiently mature to propose for adoption. We believe that the "pilot" stage could empower greater stakeholder participation in governance and could permit the direct submission of best practices to ONC or through one of our advisory committees. It could also potentially enable validation bodies to provide for validation to pilot CTEs which would provide further input in terms of the CTEs' readiness to be identified as national candidate CTEs. We could see using the HIT Policy Committee and HIT Standards Committee to provide a forum to solicit public input on identifying best practices and piloting CTEs in a manner consistent with their statutory authority. We would further envision that this process would follow the procedures and comport with the requirements of section 3004 and other relevant sections of the PHSA, for the development and adoption of standards, implementation specifications, and certification criteria.

Question 60: What process should we use to update CTEs?

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

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

2. Interoperability Conditions for Trusted Exchange – Technical Standards and Implementation Specifications Classification Process.

We believe that it would benefit the industry to include as part of the governance mechanism, a formal and transparent process to classify technical standards and implementation specifications that could ultimately be adopted within the Interoperability category of CTEs. [45] This process would be informed by the priorities set by ONC based in part on recommendations from the HIT Policy and Standards Committees through an annual review and assessment process.

Through this process, technical standards and implementation specifications could be assigned to one of three classifications:

- "Emerging" – This classification would refer to the technical standards and implementation specifications that still require additional specification and vetting by the standards development community, have not been broadly tested, have no or low adoption, and have only been implemented within a local or controlled setting.
- "Pilot" – This classification would refer to the technical standards and implementation specifications that have reached a level of specification maturity and adoption by different entities such that some entities are using them to exchange health information either in a test mode or in a limited production mode.
- "National" – This classification would refer to the technical standards and implementation that have reached a high-level of specification maturity and adoption by different entities

[45] Examples of technical standards include SMTP, S/MIME and X.509 which form one of the transport specifications we identify for satisfying CTE I-1.

such that most entities are using or are readily able to adopt and use them to exchange health information to conduct business. These technical standards would also be candidates for inclusion in applicable regulations, such as being referenced in an Interoperability CTE.

We believe the governance mechanism can and should be used to promote innovation in the health information exchange market. Therefore, we believe with the identification of the Emerging and Pilot standards and implementation specifications, the governance mechanism could encourage groups of HIT stakeholders to test, learn about, and provide feedback on those standards and implementation specifications and their readiness to be promoted to the next classification.

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?

The following figure generally illustrates the classifications discussed above. The upper right hand corner of the figure denotes standards classified as "National," indicating readiness for national adoption. We highlight the fact that a technical standard could be considered highly mature, albeit, not very adoptable (upper left portion of the figure), or conversely, a standard could also be determined to be highly adoptable, but not very technically mature (lower right portion of the figure). In such instances we would task the HIT Policy and Standards Committees with providing advice on policy and technical justifications for whether a standard with these characteristics should be put on a path toward national adoption.

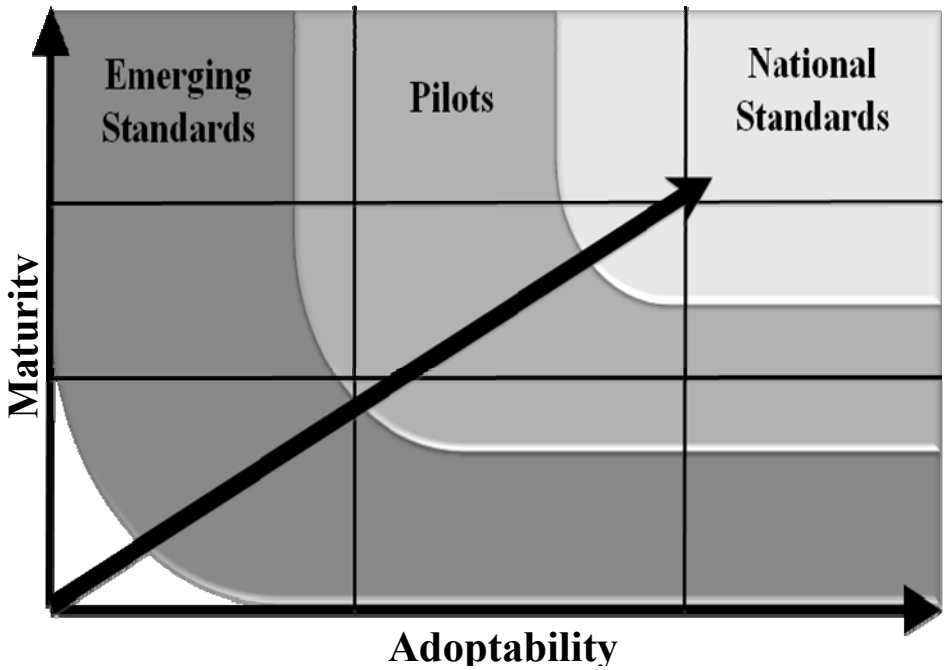

Figure 1. Standards and Implementation Specifications Classification Grid.

Technical Standards and Implementation Specifications Classification Criteria

Coupled with the annual process to identify, review, and assess standards and implementation specifications, we assume that a discrete set of objective criteria would be necessary to assess whether and when a technical standard or implementation specification should be classified differently. We believe the HIT Policy Committee would have a key role in prioritizing technical standards and implementation specifications needs and the HIT Standards Committee could have an integral role in advising ONC about how to classify such technical standards and implementation specifications. The HIT Standards Committee has had initial discussions on what classification criteria could look like, such as: maturity; market adoption, need; deployment complexity; and the maturity of the underlying technology for a given standard.

Question 64: Would this approach for classifying technical standards and implementation specification 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.

G. Economic Impact

As part of an NPRM, we would perform a regulatory impact analysis consistent with Executive Order 12866 and other applicable requirements. The focus of the RFI is to obtain public comment on what would be necessary to launch the structures, processes, and initial requirements to establish a governance mechanism for the nationwide health information network, but also interested in public comment on any publicly available data that we could subsequently use in a future NPRM's regulatory impact statement to determine the costs and benefits of such a governance mechanism.

Question 66: We encourage comment and citations to publicly available data regarding the following:

1. The potential costs of validation;
2. The potential savings to States or other organizations that could be realized with the establishment of a validation process to CTEs;
3. The potential increase in the secure exchange of health information that might result from the establishment of CTEs;
4. The potential number of entities that would seek to become NVEs; and

5. The NVE application and reporting burden associated with the conceptual proposals we discuss.

Dated: __May 10, 2012_____

David S. Muntz,

Principal Deputy National

Coordinator, Office of the National

Coordinator for Health IT.

BILLING CODE: 4150-45-P

[FR Doc. 2012-11775 Filed 05/11/2012 at 11:15 am; Publication Date: 05/15/2012]