Health IT Policy Committee

A Public Advisory Body on Health Information Technology to the National Coordinator for Health IT

April 13th, 2011

National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

Dear National Coordinator,

On December 8, 2010, the President's Council of Advisors on Science and Technology (PCAST) released a report entitled "Realizing the Full Potential of Health Information Technology to Improve Healthcare for Americans: The Path Forward." PCAST is an advisory group of the nation's leading scientists and engineers who directly advise the President and the Executive Office of the President. PCAST makes policy recommendations in the many areas where understanding of science, technology, and innovation is key to strengthening our economy and forming policy that works for the American people. In this report the Office of the National Coordinator for Health Information Technology (ONC) is directly commissioned with the task of bringing many of the report's recommendations to fruition.

ONC is at the forefront of the administration's health information technology (HIT) efforts and is a resource to the entire health system to support the adoption of health information technology and the promotion of nationwide health information exchange to improve health care. ONC is advised by two advisory committees, the HIT Policy Committee (HITPC) and the HIT Standards Committee (HITSC). The HITPC advises ONC on a policy framework for the development and adoption of a nationwide health information infrastructure and the HITSC advises ONC on standards, implementation specifications, and certification criteria for the electronic exchange and use of health information.

We, the PCAST Workgroup, have been formed by the HITPC and the HITSC and have been charged with:

- Synthesizing and analyzing the public comments and expert testimony regarding the PCAST report;
- Discussing the implications of the report and it's specific recommendations to ONC on current ONC strategies;
- Assessing the feasibility and impact of the PCAST report on ONC programs;
- Elaborating on how these recommendations could be integrated into the ONC strategic framework.

We were not asked to judge the PCAST report. Indeed, we have some members who have concerns about aspects of the PCAST report, as well as some members who support aspects of the report. The workgroup limited itself to its charge, and this letter should be viewed in that context. Our comments

in this letter should not be interpreted as endorsing or rejecting the underlying policy and/or technology recommendations in the PCAST report.

We discussed the input from the public, the feasibility and implications of the PCAST report and the PCAST recommendations' potential impact on current ONC programs. In light of the directional recommendations of the PCAST report and the status of current HIT activities, we are submitting our analysis and suggested pathways by which the ONC can help achieve the end goals revealed by PCAST for health information technology capabilities in the United States. This letter describes our analysis in the following order:

A. **Summary of the PCAST Report:** This section describes the observations made by the PCAST Workgroup regarding the overall themes of the PCAST report and the specific recommendations made to ONC by PCAST.

B. **Public Comment and Hearing:** This section summarizes what the Workgroup believes are key messages from the public regarding the recommendations made in the PCAST report as represented through public comments and through the Workgroup's public hearing.

C. **ONC Actions and End State:** This section elaborates on the Workgroup's analysis of the feasibility of achieving the end goals described by PCAST in relation to ongoing ONC activities.

D. **The First Steps on The Path Forward:** This section describes various pathways that ONC programs can take to move toward PCAST end goals within the framework of Meaningful Use Stage 2 and Stage 3.

E. **Summary Comment:** In this section, the workgroup summarizes the report.

Section A - Summary of PCAST Report

The PCAST report consists of three major recommended directions:

1. Accelerate progress toward a robust exchange of health information.

2. Establish a new exchange architecture with a *universal exchange language (UEL) and interlinked search capabilities* coupled with strong privacy and security safeguards. The exchange architecture will enable clinicians and patients to assemble a patient's data across organizational boundaries and facilitate population health.

3. Establish an evolutionary transition path from existing installations to the new exchange architecture.

The PCAST Report also describes several important technical architectural concepts, which are described in Appendix D.

Our workgroup reviewed this report carefully and also considered additional material presented by members of PCAST. We have the following observations about the PCAST report.

1. The report is intended to be directional and visionary. Although the report provides examples of technical approaches that might achieve the direction, it does not recommend a specific implementation approach.

2. The high level vision described in the report is generally consistent with ONC's strategic framework. As described in the strategic framework, information exchange is a necessary part of the learning health system.

3. The PCAST report does not describe a complete solution for healthcare information exchange. A complete solution has many components, and the PCAST architecture represents some of those components. The transactions that are commonly called "push transactions" represent different exchange components that are not described in the PCAST report. (These push transactions involve transmitting certain groupings of data elements from one provider entity to another provider entity.) We believe that these push transactions do not need to be replaced by the PCAST architecture. In addition, ONC is involved with many information exchange initiatives, such as NwHIN Exchange, HIE organizations, vendor exchange efforts, NHIN Direct Project, Beacon Communities, and the SHARP projects. These initiatives will continue to play a critically important role as they create or evaluate building block components, and they provide operational experience.

4. The PCAST report describes a vision for a new information exchange architecture--an architecture that is patient- centered rather than institution-centered - an architecture where the data to be exchanged is attached to persistent metadata tags describing attributes, provenance and any necessary privacy protections and exposed to query/response services. This architecture is intended to support a broad range of information exchange activities and purposes including patient treatment as well as public health surveillance and biomedical research. For example, enabling a clinician to quickly pull together the information they need about a patient to make a clinical decision or enabling a researcher to identify a potential cohort for a clinical study. Those types of query/response or analyses activities have not yet been addressed with meaningful use and certification regulations.

Section B - Public Comment and Hearing

On December 8, 2010, ONC requested public comment on a series of questions related to the PCAST report. On February 15, 2011, this workgroup held public hearings with various stakeholders on the report. Based on our review of these comments, we have the following general observations:

1. When compared with today's systems and approaches, the PCAST report makes novel recommendations that are <u>difficult to reconcile</u> without operational examples and concrete plans.

2. There is an <u>absence of consensus</u> about the architectural approach described in the PCAST report. Some stakeholders believe that the current standards for exchange are the only approach that is needed and practical, because they focus on workflow and processes. Other stakeholders are excited about the new exchange architecture and are fully committed to its

implementation. It is not surprising that there would be an absence of consensus. We would not expect an entire industry to immediately accept a new exchange architecture based solely on the publication of a single report.

3. The PCAST report offers a technical approach for honoring patients' granular privacy preferences which can be expressed for individual data elements to be exchanged. While there is support for the additional patient privacy flexibility and, also, greater patient access, substantial privacy and security concerns have been expressed. Among the concerns are the feasibility of patients meaningfully exercising highly granular privacy controls and the effect of such controls on clinical care.

4. Timeframe (2013) is a major concern. The public comments reflect the stresses experienced by providers and vendors as they attempt to address existing meaningful use requirements coupled with other industry challenges, which include the ASC X12 v.5010 transition in 2012 and the ICD-10 transition in 2013.

The public comments also included concerns that a shift in emphasis to the new exchange architecture might detract from other ONC programs. A more detailed description of the feedback can be found in Appendix B.

The public comments had a significant impact on this report from the workgroup.

Section C - PCAST End State and ONC Actions

In this section, the workgroup discusses alternate long-term actions that ONC might take to achieve the PCAST end state vision.

Description of PCAST End State Vision

The PCAST end state vision is based upon the new exchange architecture, which consists of a *universal exchange language and interlinked search capabilities* coupled with strong privacy and security safeguards. From the viewpoint of participants in the healthcare system, this architecture is intended to facilitate the following vision.

1. Every American will have electronic health records and will have the ability to exercise privacy preferences for how those records are accessed, consistent with law and policy.

2. Subject to privacy and security rules, a clinician will be able to view all patient data that is available and necessary for treatment. The data will be available across organizational boundaries.

3. Subject to privacy and security rules, authorized researchers and public health officials will be able to leverage patient data in order to perform multi-patient, multi-entity analyses.

Impact on Policies and Strategies

The PCAST end state vision is generally consistent with the concepts of the Learning Health System as described in ONC's strategic framework. The new exchange architecture introduces technical directions that raise new policy, regulatory, and governance issues, however. Appendix C contains a preliminary list of policy issues that need review and describes the implications of those policy decisions. The PCAST end-state vision will impact three fundamental areas of policy and strategy:

1. Privacy and Security: The PCAST report describes the technical capability to attach patient privacy preferences to individual data elements that are to be exchanged. The extent of that granularity and the practicality of data element privacy choices are topics for review. Corresponding policies need to be created that facilitate the concepts of dynamic and meaningful choices as recommended by the HIT Policy committee. In addition, the extent of granularity impacts the quantity and utility of metadata in the Data Element Access Services (DEAS), which represents another privacy issue to be considered.

The granular privacy issue has broad implications on consumer acceptance, provider adoption, clinical functions, and administrative processes.

2. Large, multi-patient, multi-entity datasets and analyses: The PCAST report contemplates leveraging granular health data for data analyses. The impact on clinical care as well as the impact on multi-patient analyses of an architecture that uses data for multiple purposes needs to be investigated. Similarly, it should be determined whether the use of data for multiple purposes conflicts with other key policy interests, including privacy. The efficacy of the new exchange architecture for analytical work also needs to be determined.

A foundational issue is to identify and prioritize the clinical and analytical goals of health information exchange.

This policy issue has structural implications for the exchange architecture. The prioritization of "secondary uses" of data could impact the extent that information is exchanged at an atomic level and the structure of indexes and directories.

3. Governance. There are many governance questions related to the record locator services (DEAS) and to the end-state vision described in the PCAST report. For example: Who is responsible for the administration of DEAS? How do we assure data quality? How do we assure metadata quality? The PCAST report says that DEAS accesses would be audited, but who will monitor this audit trail and enforce compliance with policies? ONC has already started a process to establish governance for the NWHIN, and the PCAST end vision will impact that effort.

NWHIN governance will be critically important to the success of the PCAST vision.

Impact on Standards, Information Exchange

The PCAST report provides many directional concepts with examples of enabling technology, but it stopped short of recommending a specific technical implementation. As described in the previous section, various policy decisions will impact the ultimate technical implementation. The workgroup created a task force of experts to illustrate alternative technical implementation approaches. Using the technical concepts described in Appendix D, the task force created three use cases and a table to place the related technical designs side by side. As a result of this work, the task force identified 15 components, e.g., standards, services, application capabilities and related policies that need to be defined or created in order to implement the PCAST vision. *The task force showed that it is possible to implement the new exchange architecture in a series of incremental steps.* In other words, instead of being forced to pick one complete implementation, it is possible to start with a first partial implementation and incrementally advance to the third, which represents implementation of the PCAST end-to-end state. The use cases and the table of levels of exchange are described in Appendix E. Through this exercise, we learned:

1. There is substantial value in having a defined architectural goal. The knowledge of an end-state, coupled with a set of technical concepts and principles, facilitates decision making and helps illuminate a path forward.

2. The technical decisions are inter-related, as are policy decisions. As a basic development principle, a holistic view is needed.

3. In addition to the policy questions, there are areas where there are unknowns. We are unaware of any real-world environments (either in healthcare or other sectors) where the combinations of technologies envisioned for the end-state have been placed into operation. Another basic principle is to create operational test-beds prior to national deployment of new combinations of technologies.

Suggested Deployment Models

The workgroup was asked to provide alternative models that describe how ONC might aggressively pursue the PCAST vision. Assuming that technical development decisions are coordinated with policy decisions, we see three possible deployment models: top-down, bottom-up and middle-out. In each deployment model, the tasks that need to be accomplished probably include the following activities:

a. Policy questions are resolved.
b. Each of the 15 components of the technical framework is defined. This requires specifying identifiers, formats and protocols (IFaPs):
    1) Identifiers for all the important objects and metadata required to implement the 15 components
    2) Formats for objects including, but not limited to, the UEL syntax
    3) Protocols by which the components interact.
c. A governance body is created
d. DEAS operators are created
e. Incentives to participate created through appropriate government levers such as meaningful use measures.

As will be described below, the three implementation models differ in the sources of funding and the degree to which various activities are performed by ONC.

1. Top-Down Model: This model involves full direction setting by ONC and represents the most aggressive deployment approach. For total deployment, this approach involves ONC making all of the necessary decisions for the activities described above.

Resources: The workgroup observes that ONC lacks the core competencies to make the necessary technical decisions for this model. The top-down approach will require significant additional financial resources for ONC to obtain expanded technical capabilities, manage new pilot projects, resolve unanswered policy questions, and create DEAS organizations. In order to obtain the additional funding, other ONC activities will need to be displaced, and/or, other HHS activities need to be displaced. As

described in the PCAST report, a rapid deployment will require providers and hospitals to obtain middleware, which is expected to increase costs.

Benefits and Risks: While the Top-Down Approach has the benefit of deployment speed, it has the following risks:

a. Technical risks: Making all technical decisions on an accelerated time table and immediately specifying a broad range of standards might result in decisions that are regretted later.
b. Acceptance risk: Implementation of a national technology without industry support might result in a low level of adoption.
c. Rapid deployment efforts may be counter-productive. In an increasingly complex HIT environment, additional meaningful use focus on technology coupled with increased EHR costs could discourage participation in the voluntary phase of HITECH.

2. Bottom Up Model: With this model, the private sector sets the direction for the development of exchange technology. Once tested and market-proven exchange technologies emerge, ONC can create an exchange framework that involves these components. At least one major EHR vendor is discussing building their own DEAS for its customers. That independent effort is typical of the Bottom Up model and indicates that it may have already started.

Possible actions involved with this model are:

1. Grants from SBIR or other federal programs that provide seed funds to vendors.
2. EHR contracting requirements at the VA, DoD, IHS, or other federal health delivery networks that would require vendors to perform in accordance with the new exchange architecture.
3. ONC grants to encourage open source implementations of important tools or technologies.
4. Resolution of policy questions that may arise from this model.

Benefits and Risks: Proponents of a bottom-up model believe that this model has minimal technical risks because the marketplace is an efficient way to identify effective technologies. Others believe, however, in the absence of standards, technical risks exist because various vendor-supplied approaches may not be nationally interoperable and might not lead directly to a single architectural approach.

Resources The Bottom Up method requires the least resources.

3. The Middle-Out Model ("Building Blocks"): With this model, ONC will identify policies and standards for technological building blocks for exchange that must be achieved in an incremental fashion (built into Meaningful Use stages, ONC standards and certification criteria), while a public-private partnership works in parallel to create the national exchange framework. With this approach, a minimal set of standards and protocols are initially identified and, following operational experience, incrementally advanced. If ONC decides to pursue the Middle-Out Model, it will need to determine the set of standards and protocols that represent the most efficient initial activities. Appendix F describes a few alternatives along with a table that compares the three deployment models.

The efforts to create building blocks may be performed through the S&I Framework, with the HIT Policy and Standards Committees recommending policy and standards respectively. These standardization efforts would be synchronized with pilot project ("test bed") activities and, also, appropriately timed to meet regulatory deadlines in support of ONC goals for the stages of meaningful use.

Benefits and Risks: This approach has the following benefits:

a. It requires fewer new ONC resources and is consistent with previous ONC actions.
b. Technology risks are minimized, because there is parallel public-private development.
c. It is consistent with the overall approach for the new exchange architecture.

It is difficult to predict the relative speed of each model. While a Top-Down approach would appear to be the fastest, proponents of the Middle-Out model express the opinion that a minimalist standards approach represents the most effective deployment approach for ONC. They support their opinion with comparisons to the development of the Internet, which they say similarly involved through the iterative release of minimalist standards and protocols.

These three models should not be viewed as separate, isolated choices. It is possible that a combination of models can be used. For example, the record locator services (DEAS) involve complex technical challenges and the thorniest policy issues. For the DEAS, it is possible that vendors (through a "bottom-up" approach) will build successful operational systems or that pilot projects might develop multiple successful operational concepts. *It is also possible that an architecture can be created that does not require an external DEAS.* A mixture of deployment models might be used. The Middle Out approach could be used to identify the foundation standards (e.g. data, metadata, security, and the UEL) that enable multiple operational tests of DEAS concepts.

Section D - The First Steps on the Path Forward

Our implementation task force reviewed the technical requirements of a complete "end-to-end" implementation that would involve all components of the PCAST vision. Such an implementation is described as level #3 in the implementation table in Appendix E. The workgroup concludes that it is not feasible to include a complete "end-to-end" implementation in meaningful use stage two (2013). The following factors led to this conclusion:

1. With many unknown aspects of a possible implementation, there is inadequate time to prepare detailed regulations and testing criteria.

2. The workgroup was sensitive to the concerns expressed by many stakeholders about competing time pressures for activities like ICD-10 with existing 2013 commitments.

3. Greater industry support and greater understanding is needed before a new, national technology effort is launched.

While the workgroup concluded that a complete "end-to-end" implementation involving all functions is not feasible for Stage 2, it is possible to implement the new exchange architecture in an incremental fashion. The implementation table in Appendix E describes one possible progression for implementing the new exchange architecture. The progression includes the following progressive and sequential steps:

1. Define UEL and initial data and metadata standards.
2. Create initial record locator (DEAS) concepts with minimal metadata, and expand UEL; data, and metadata standards.
3. Expand to support additional granularity and further expand UEL, data, and metadata standards, and capabilities to perform complex searches.

These steps need to be coordinated with policy development. For example, as stated earlier, the extent of granularity has significant policy implications. The sequence suggested in Appendix E provides a path for ONC to incrementally advance the PCAST vision and incrementally increase the complexity of the transactions involved. Each progression builds on the experience and the policies of the previous steps. The workgroup believes that the new exchange architecture has the flexibility to enable this type of progression.

With an incremental approach, first steps can be taken in Stage 2 Meaningful Use within existing policy and with proven technology. At the same time, test bed projects can be vigorously pursued to test promising combinations of technology and policy end-to-end. The successful combinations can then be incorporated in Stage 3 Meaningful Use.

First Step: Stage 2 of Meaningful Use

The workgroup sees the following possible alternatives for Stage 2:

1. Patient Portal and Patient Access to Data: Consistent with the PCAST report's emphasis on patient engagement, Stage 2 of Meaningful Use could contain metrics for the use and promotion of Patient Portals. In addition to providing patients with access to their information, the portals could give patients an option to obtain an electronic copy of their data, using tagged data elements. Two alternate approaches are suggested:

a. Patients may download their data directly. In this alternative, the data is sent as a CCD or a CCR with metadata tags. At their option, the patient could subsequently upload their data into

a PHR. This download/upload approach is a common functionality that is made available to consumers in the finance industry.

b. Patients may request that their provider transmit their data directly to a PHR (or other entity). This alternative would similarly use tagged data elements, but would also include the use of transport protocols (probably using standards identified through the Direct Project).

With either approach, an initial forward step is taken toward the new exchange architecture. In effect, Version Zero of the UEL is defined with an initial "UEL wrapper" that consists of a minimal set of metadata that is attached to a CCD or CCR transaction. The technical requirements are described as "Level One" in the implementation table and as Use Case One in Appendix E.

This approach has the following benefits:

a. As recommended by the PCAST report, ONC will be signaling that tagged data elements are required for Meaningful.
b. It gives patients access to an electronic copy of their data and the capability to request that a copy be sent to a third party (as required by law).
c. The PHR vendors might independently become a resource that could create the types of innovation that the PCAST report envisions.

In general, here are the steps that ONC can take to implement this suggestion:

a. Define the UEL Syntax: ONC can take a first step toward the PCAST vision by asking the Standards Committee to define the syntax of the "Version Zero" Universal Exchange Language. Progress can be made rapidly if the XML syntax for the UEL is the same or a subset of what is currently used by CCD and CCR. As part of this decision, naming standards for the metadata tags could be determined. The use of any specific naming conventions or syntax does not necessarily determine which names or syntax will be used in the future. The technology has sufficient flexibility that these initial decisions will not become decisions that might ultimately be regretted.

b. Include in Stage 2 certification the capability to transport data in the Version Zero UEL. The first alternative could then become part of the menu of Meaningful Use choices.

c. Complete a set of policies relevant to patient access to data in an EHR and the ability to download, including directly to a PHR.

d. Simultaneously with Stage 2, but not as a requirement for creating the certification criteria, ONC could commission a Naming Authority to manage naming and versioning for that syntax and the various data structure and semantic standards that will be utilized within the UEL.

2. Certification criteria for exchange transaction. As another alternative, using the same series of steps, ONC can use Stage 2 certification criteria to identify metadata standards for other specific stage 2 transactions.

For each of these two alternatives, the workgroup, which includes members of the HIT Standards Committee, believes that the necessary technical decisions can be made with sufficient time to be tested and included in Stage 2 of Meaningful Use. The workgroup believes that this approach to Stage 2 of Meaningful Use is consistent with the PCAST report's direction to act boldly.

Stage 2 Path of Least Regret

We were asked to help ensure that there were no information exchange transactions proposed for Stage 2 that would be regretted in the future, as the new exchange architecture is implemented. As a result, we reviewed the transactions that have been proposed for Stage 2 meaningful use: e-prescribing, lab results reporting, immunization reporting, providing discharge summaries, and providing summary records. These transactions are either "push" transactions or, in the case of e-Prescribing, expansion of transactions that are already widely adopted. As a result, these proposed stage 2 MU transactions do not conflict with PCAST implementation efforts.

In addition, the following proposed Stage 2 activities, are important and valuable steps. Accelerated emphasis is consistent with the PCAST recommendations:

a. Patient Identity Matching initiatives
b. Vocabulary Efforts
c. Polices for trusted Intermediaries
d. Patient/User identity assurance and authentication
e. Communications protocols (e.g. the Direct Project)
f. Security standards and policies
g. Privacy policies

Continued efforts through the NwHIN Exchange, HIE Organizations, vendor exchange efforts, the Direct Project, Beacon Communities, and SHARP grants will create critically important building block concepts and provide operational experience.

Next Steps

Getting ready for Meaningful Use Stage 3:

1. With the Policy Committee's assistance, ONC can develop more specific privacy and security policies that will build and maintain public trust in the new exchange architecture. One focus of this effort might involve a public discussion of the record locator services (DEAS) and whether there are alternative architectures that eliminate the need for separate indexing entities or minimize the extent of external indexes.

2. With the HIT Standards Committee's assistance, ONC can develop the additional syntactic and semantic standards to support the components needed for the next levels of the Implementation Framework.

These two activities would open the way to supporting projects to test, end-to-end, promising combinations of technology and policy. A test-bed involving the VA, DoD, IHS, and NwHIN Exchange might be particularly useful. Test beds ("pilot projects") are needed for the DEAS and granular privacy choices. The number and intensity of these pilot projects will impact the speed by which progress can be made.

These test-bed pilot projects and public discussions can also help address the problems that arise from the absence of consensus within the industry. Before any new, major, national implementation effort can succeed, it is important that there is both industry understanding and support for that effort. Multiple successful pilot projects will make a major contribution to creating the necessary support. *In order to be considered for Stage 3 of Meaningful Use, it is necessary that pilot projects be operational no later than October 1, 2012 so that there will be at least six to nine months of operational experience prior to the date when Stage 3 decisions must be made*. Each test-bed pilot project should have success criteria established in advance. Such success criteria should, at the minimum,

1. Measure the frequency and the perceived effectiveness of the usage of the exchange process by clinicians.
2. Measure the experience of consumers, including (but not limited to) the management of granular privacy choices.
3. Using real-world examples, determine the usefulness of the architecture for population analyses and other multi-patient analyses.

The successful approaches from the test-beds could then be incorporated into Stage 3.

We believe that this incremental approach is entirely consistent with the PCAST's report's direction to act boldly and is also consistent with the report's direction for an evolutionary path that does not replace existing EHR systems.

Other Policy Levers

Progress should not be solely limited to the regulations that are written related to the various Meaningful Use stages. ONC has other policy levers that can be used to influence progress. These include:

1. The S&I framework: The identification of standards and infrastructure components has a major influence on vendors and on other healthcare constituents.

2. NWHIN Governance: The governance function can be used to promulgate best privacy practices and to implement standards, as well as to validate the usage of security and other infrastructure technologies.

3. RECs: The regional extension centers can play a role in educating providers in the new exchange architecture and assisting with its adoption.

4. Granting Authority: ONC can use its granting authority to encourage the use of various pilot projects or to encourage existing grantees to participate in pilot (test bed) projects. In particular, HIE organizations might be used for various pilot testing projects involving the DEAS. In addition, it may be beneficial to consider organizations that have not previously received grants.

5. Certification Criteria: Certification criteria can be written to advance the new exchange architecture. This approach might be particularly useful for infrastructure items involving security and communications.

6. Bully Pulpit: All of ONC's activities are closely watched. Discussions about policies and standards can impact the future actions of many industry players. Actions to organize public workshops and open discussions on various information exchange and related privacy policies have an impact.

Section E - Summary Comment

This workgroup is a diverse group of individuals with a range of opinions about the PCAST report. This document reflects our consensus view and we wish to emphasize the following three points:

1. The PCAST report describes a national use of advanced technology. It provides a compelling vision for how that technology could be beneficially used as an important aspect of the learning health system

2. There are major policy and operational feasibility concerns with the proposed technology.

3. Aggressive and rapid progress is possible only with an incremental test-bed approach. Large operational tests are needed that resolve the policy and feasibility concerns.

The ultimate challenge is to find the correct balance between the inspirational goals of the PCAST report and the practical realities of a nationwide deployment of electronic health records. We respectfully submit this letter hoping that it will assist ONC in achieving that balance.

Sincerely yours,

/s/

Paul Egerman
Chair – PCAST Workgroup

Sincerely yours,

/s/

Bill Stead
Co-Chair– PCAST Workgroup

Appendix A - Members of Workgroup

Member	Organization
Chairs	
Paul Egerman, Chair	
William Stead, Vice Chair	Vanderbilt University
Members	
Dixie Baker	SAIC
Hunt Blair	Vermont HIE
Tim Elwell	Misys Open Source Solutions ("MOSS") LLC
Carl A. Gunter	University of Illinois
John Halamka	Beth Israel Deaconess Medical Center, HMS
Leslie Harris	Center for Democracy & Technology
Stan Huff	Intermountain Healthcare
Robert Kahn	Corporation for National Research Initiatives
Gary Marchionini	University of North Carolina
Stephen Ondra	Office of Science & Technology Policy
Jonathan Perlin	Hospital Corporation of America
Richard Platt	Harvard Pilgrim Health Care Institute And Harvard Medical School
Wes Rishel	Gartner
Mark A. Rothstein	University of Louisville School of Medicine
Steve Stack	American Medical Association
Eileen Twiggs	Planned Parenthood Federation of America

Acknowledgements

The PCAST Workgroup would like to thank the following individuals who provided us with assistance in preparing this report:

Office of National Coordinator

Farzad Mostashari

Doug Fridsma

Jodi Daniels

Charles Friedman

Joy Pritts

Judy Sparrow

Jamie Skipper

Members of PCAST

Christine Cassel

Craig Mundie

William Press

Appendix B - Summary of Public Comments

Part A. Summary of PCAST RFI Public Comments

The Request for Information (RFI) yielded a rich and descriptive collection of thoughts from industry stakeholders regarding the PCAST report's recommendations. The major concepts and messages that emerged from the public comments are as follows:

1. Timelines. Many commenters supported the PCAST recommendations that focused on increasing information exchange capacity before meaningful use Stage 2. The majority of commenters, however, expressed concerns about the effects of attempting to fully implement the recommendations in the midst of rolling out Stages 2 and 3 along with other changing standards such as the move from ICD-9 to ICD-10. They contended that there could be negative effects on patient safety. Many commenters suggested that the report's recommendations be a long term strategy rather than an immediate deviation from the current groundwork that has already been laid.

2. Effects on ONC Programs. The majority of commenters encouraged ONC to leverage the success of ongoing programs and avoid reinventing the wheel in the midst of the EHR incentive programs. Many stated that fully implementing the PCAST report's recommendations would require redesigning many of the ongoing federal HIT grants and contracts which would impose substantial costs to current participants. Some suggested that ONC begin with pilots to develop and test PCAST technology solutions before being moving into wider implementation.

3. The Implementation of PCAST Recommendations. Commenters generally agreed that health information exchanges (HIEs) and the electronic exchange of health information should be the focus of future stages of meaningful use. Regarding the exchange of "atomic level" data, many agreed with the necessity of a Data Element Access Services (DEAS) structure, but recommended that such a program begin with pilot testing that takes into account patient-linking and public trust issues.

4. Privacy and Security. Many commenters supported the concept of giving patients granular consent as envisioned in the PCAST report. However, many expressed concern that tagging patient privacy preferences to the data would lead to a static, rather than a dynamic, data control environment that prevented patients from updating their privacy preferences once the data was released. The research community largely supported PCAST's concept of creating a subset of de-identified data for the purpose research, although others were skeptical that data could truly be de-identified.

5. Standards. Many commenters echoed that belief that ONC should learn from and leverage existing standards that incorporate metadata concepts. Some commenters asserted that ONC should pursue the approach outlined in the PCAST report because current standards do not allow for innovation, flexibility, or scalability and that today's predominantly document-centric environment would not support PCAST's vision. Others contended that the report's interoperability and data liquidity goals could be met with existing and emerging standards.

Part B. Summary of Hearing Panels' Discussion

On February 15, 2011, the workgroup held a public hearing and invited industry stakeholders to provide input. These stakeholders represented:

- Health information exchange representatives
- Healthcare and health IT experts
- Patients and health care consumer advocates
- Privacy advocates
- Representatives for population health
- Providers and hospitals, including those using various types of electronic health records and middleware
- Technical experts on EHRs and EHR programming and coding

Each of these stakeholders formed a panel, and the feedback is summarized for each panel.

Panel 1 – Health Information Exchange and Healthcare Stakeholders

1. Concerns about security/consent model. Chapter V of the PCAST report describes an example of a method by which the operator of a DEAS could enforce patient's consent preferences. The approach is predicated on the use of metadata tagging of data elements and the use of encryption in a manner often associated with digital rights management (DRM). One sort of tag associated with a data element would include an encrypted statement of the patient's preferences for who might receive the data. This information along with the receiver's identity credentials would be reviewed by DEAS and the DEAS would only release the cryptographic key to unlock the data if the intended use was consistent with patient preference. The DEAS would have the ability to release the data as "identified" or "de-identified" according to the combination of requester and patient preferences.

A primary concern was that such a technology (or any other) is insufficient absent a framework of policy levers to enforce trust along the way and to ensure that patients consent for the release of data was revocable at any time. A secondary concern was that DRM techniques had not been effective in protecting intellectual property but had served as a barrier to innovative ways to use data.

2. Concerns about the use of un-normalized data. Several concerns were expressed about the notion that the DEAS would offer up data that had not been normalized to standard codes and other semantic characteristics of data. It was noted that successful health information exchange organizations today usually offer mapping services to support data suppliers in providing data in a semantically acceptable manner.

3. Concerns about losing context information inherent in document structure. At page 72 the PCAST Report says

> While [the HL7 CDA document approach] shares many features with the universal exchange language that we envisage, it lacks many others. In particular, it perpetuates the record-centric notion that data elements should "live" inside documents (albeit metadata tagged). We think that a universal exchange language must facilitate the exchange of metadata tagged elements at a more atomic and disaggregated level, so that their varied assembly into documents or reports can itself be a robust, entrepreneurial marketplace of applications.

A number of participants expressed substantial concern that isolated information taken out of context from a document would be subject to substantial misinterpretation. Others agreed, but acknowledged that many kinds of data are routinely abstracted from documents where the context is unlikely to change the interpretation.

4. Concern about the implied federated architecture. Concerns were expressed about the interpretation that data would remain in the source system or a content system operated by the source organization for the purpose of offering data to the DEAS. The commenters noted that healthcare delivery organization have historically been unwilling or unable to provide service levels for remote access that would be acceptable for Google-like indexing and retrieval on demand. Because the provision of such service is not central to the business model of health delivery organizations (HDOs), they prioritize bandwidth and staff support time to other applications. Some of them may no longer be in business at a time when historical information is sought. The closest analog to a DEAS in current practice is a health information exchange. A number of HIEs have met this challenge by providing centralized data storage or "proxy servers" dedicated to the data of a particular HDO but operated by the HIE.

5. Strong support for metadata tagging that describes data provenance. Numerous panel members and committee members supported the notion that data that is being retrieved should, to the maximum extents possible be tagged with information that tracks how it has been passed from system to system.

Panel 2 – Patients/ Consumers/ Privacy Advocates

1. Consent is essential but not sufficient. The PCAST report places great reliance on consent to achieve privacy protection. Although patients should have a right to be informed about health information exchange procedures and their participation in them, consent alone is insufficient. Many patients lack the health literacy, cognition, language ability, or other attributes needed for meaningful consent. Therefore, a range of fair information practices and regulatory controls also are needed.

2. Segmentation, rather than granular controls, should be used. A key element of the PCAST privacy strategy is the use of granular controls, at an atomic (data element) level. The panel members opposed

the use of granular controls, which they considered impractical. Instead, methods of segmentation of information by category (e.g., mental health) should be developed.

3. Privacy preferences should be dynamic. Patient health status, societal attitudes, and patient preferences all change over time, and therefore patients should have the ability to revise their privacy preferences to reflect these changes. The panel members had concerns that persistent metadata tags may result in inflexible privacy preferences.

4. De-identification is a problematic privacy strategy. There are technical problems in adequately de-identifying health information and preventing the information from being re-identified. Even if de-identification were technically possible, the use of individual health information without the knowledge of or consent by patients would infringe on their substantial autonomy interests.

5. Clinical applications are most important. The first priority should be to design a system that best achieves information exchange essential to treatment. Panel members expressed considerable unease that a PCAST-inspired system would facilitate the use of information for research and other secondary uses to the detriment of privacy interests or applications for treatment.

6. Many other privacy issues have yet to be addressed. Although wide-ranging, the panel discussions did not consider all of the issues related to privacy. The minimum level of detail in the PCAST report regarding privacy did not permit a consideration of all of the possible consequences. In particular, the DEAS, a new concept, should be pilot tested to assure the public that it would not compromise privacy. Data segmentation is another area in need of further research. It is also essential to research public attitudes about options to protect health privacy and to undertake extensive efforts involving provider and patient education.

Panel 3 – Population Health & Clinical Research

The panel highlighted the differences between the data needed for population health and clinical research and the data needed to care for an individual patient. The discussion reflected that the PCAST report was largely silent on the following issues:

1. Population health and clinical research require persistent record sets that are curated for the anticipated use.
    a. It is essential to bring together knowledge of the question being asked with knowledge of the data (meaning, completeness, accuracy, etc.) to know if the data can contribute to a meaningful answer to the question.
    b. Correct interpretation of data requires participation of the originator because of differences in how terms are used and data is captured. Continued development of semantic standards is essential and will decrease but not eliminate this dependence.
    c. Data captured in the course of clinical care is observational. Observational clinical data can be used to answer certain questions. Population health and clinical trials require additional types of data.
    d. Research data models reflect study design, not the characteristics of the data.

e. Distributed data analysis has proven effective for population health studies. In distributed analysis, a common data model is agreed to among participating sites, each site transforms local data into the common model but continue to hold it locally, and extract statistical data that can be aggregated across sites.
f. PCAST does not preclude and can support distributed data analysis.

2. Population studies require inclusion of the complete population of interest and all data needed to identify benefit and risk of an intervention. For example, how many are eligible, of those how many received it, of those how many had signs of benefit, and how many had signs of adverse events.
    a. Granular consent and opt out by data suppliers and individuals would be problematic.
    b. Polices are needed to continue support for use for public health.
3. De-identification is problematic
    a. The more complete a data set is, the more difficult it is to de-identify.
    b. Strategies that reduce re-identification risk may prevent use for population health.
    c. Institutional Review Boards will continue to be essential governors of data use for research.

Panel 4 - Providers and Hospitals

Panel #4 consisted of hospital/health system and primary care/community health providers.

PCAST-specific:

Meta-data privacy tag concerns: Meta-data privacy tags could unintentionally impede usual and customary flow of data necessary for routine data exchange needs. Routine quality improvement efforts, internal audit functions, and other operational requirements could be hindered depending on what is deemed to be internal versus information exchange (e.g., if a health system subcontracts with an outside vendor to provide ongoing compliance review privacy meta-data tags could unintentionally interfere with an internal function performed by an external vendor). Operationally, patient preferences could differ based on stage of receiving care – a patient could provide different consent at different times within a single episode of care, across care episodes, or in different settings. This assumes, of course, that the patient even understands what they are consenting to which is far from certain. On the other hand, meta-data tags could ensure that certain necessary contextual data is associated with the underlying data.

Middleware as partial bridge: It is a viable solution and the only way to achieve the goals in such a small period of time i.e. by 2013, but middleware is costly and installation is time-consuming. One can tag results data and can expand on that methodology. There's challenge because some existing systems do not have such middleware technology. Other initiatives like ICD10 will make it challenging to adopt such middleware technology. Things like taxonomy, patient matching, policies, and workflows are more difficult to implement than adopting the XML language itself. One recommendation is not pursue it aggressively in a short time frame. In contrast, middleware is not a viable solution to ensure front end of system, this approach does not suffice, but it does in the back end.

Timeline (2013) too aggressive: Meeting PCAST vision by 2013 is not feasible especially with other initiatives like MU, ICD10, and 5010 changes. It might be attainable if those other initiatives are kept aside, but people will not be willing to do so. Also, great investment has already been made in MU stages 1, 2, & 3. How are these reconciled without destructive disruption?

PCAST-related but HIE generalized:

Patient matching remains problematic: This item was raised as a real and enduring concern. Despite sophisticated matching algorithms and ongoing efforts the problems with not finding needed data or, possibly worse, finding the wrong data and merging it incorrectly with other data remains a big problem. This is not uniquely germane to PCAST but it remains an unresolved challenge that requires ongoing attention in any HIE context, PCAST or otherwise.

Novel PHR use could spur HIT adoption: We need to get people to want the technology, understand or appreciate the technology, and have the ability to manage health along with providers using HIT. The use of PHRs for appointment scheduling, secure messaging, patient reminders, etc... could spur patient engagement and foster both patient and provider uptake.

Panel 5 - Technology Implications

Panel #5 consisted of EHR Vendors, Open Source Vendors, and in-house (self-developed) organizations.

Context is important: If data is transmitted in a format that is a subset, summary or data atomic abstract of an original encounter, it is important to include enough data and metadata to retain the meaning of the original information. For example, if the atom is a problem list entry of "coronary artery disease," it is important to know if that clinical context is "family history of," "rule out," "confirmed by stress testing," "or risk of due to diet/smoking/obesity/lethargy." Reusing data for a purpose other than the original reason that the data was gathered (i.e., do research on data gathered for clinical care) is especially problematic unless context is maintained. Information models provide frameworks to maintain context. Explicit representation of context must be integrated into an evolving Universal Exchange Language and may require specification of an information model.

Timeframe (2013) is a major concern. We must evaluate the burden and timeframe and priority of implementing PCAST recommendations in the context of existing meaningful use and ICD10/5010 projects.

Data normalization (the application of controlled terminology) should be applied as close to the source as possible - It is far easier to maintain the original context of the data if it is captured by clinicians during data entry using controlled terminology with appropriate granularity. For example, gathering structured systolic and diastolic blood pressure with known units of measure via a specified methodology (i.e., "120/80 mmHg from the right arm while sitting" is easier to reuse than "Blood Pressure of 120.")

The size of a data atom should be that set of information which makes sense for the purpose intended - an atom could be a single data field, a collection of data fields, or an entire document.

The container used to send the data should be separated from the ontologism and vocabularies used within the container to convey meaning - The Universal Exchange Language (UEL) should not include its own specific vocabulary, but existing separate vocabularies should be used to convey meaning of data transmitted. Data transmitted in the UEL may be structured or unstructured. Structured data may or may not be terminology controlled. We do not need to wait for perfect vocabularies to provide controlled terminologies for all structured data. These vocabulary concepts are consistent with the recommendations of the PCAST report.

Data quality is highly variable - we need to know the provenance of the data including who gathered it, in what workflow, and for what purpose to help convey the quality of the data gathered.

Open source development should be highlighted as an example of how software development may be accelerated and how standards, architectures, designs, and approaches may be implemented using a transparent process. A possible result of using this process is reduced cost.

Appendix C - Policy Issues

The workgroup identified the following issues and strategies that are candidates for policy development related to the new exchange architecture.

1. Granular choice:

NCVHS and the HIT Policy Committee have both addressed issues related to the granularity of choice. The following observations are limited to the granular architectural approach described in the PCAST report.

The PCAST report describes the use of metadata for expressing persistent privacy preferences for individual data elements. Corresponding policies need to be created that facilitate the dynamic and meaningful choices that were recommended by the HIT Policy committee. According to that recommendation, in order to exercise "meaningful choice," consumers need to understand privacy choices and the impact of those choices on their care. As a result, the extent of granularity and the practicality of data element privacy choices are topics for review. The burden on both patients and providers to manage data element consent choices also should be reviewed. Providers' responsibilities as record holders are impacted by these policy decisions. The relationship to the NCVHS recommendations, the HIT Policy Committee recommendations, as well as the public comments encouraging segmentation should also be reviewed.

This granular privacy issue is critically important to the success of the HITECH initiative. It has broad implications on consumer acceptance, provider adoption, clinical functions, and administrative processes.

2. Relationship between EHR and PHR and Control of the Record.

The PCAST report places emphasis on the use and benefits of PHR systems. Indeed, PHRs are mentioned fourteen times in the report. If the PCAST architecture is implemented in such a way that EHR systems use PHR systems as a source to retrieve and deliver metadata tagged patient information, then policy issues might arise. Under those circumstances, ONC might examine the relationship between the PHR and the EHR to determine whether privacy and security policies need to be expanded to cover PHRs, or if new policy is needed.

An alternate approach would involve defining PHRs and EHRs as separate record-systems that are not merged together. (This alternate approach is generally consistent with the treatment in current law,

except where the PHR is offered on behalf of the provider). With this alternative approach, PHR systems would be maintained by patients, while EHR systems would be maintained by providers, and each would serve different functions. With this approach, a patient would have an option to list their PHR in a record locator service (DEAS) instead of their EHR, and providers would know whether they are viewing PHR records or EHR records. This alternate approach has implications for the granular privacy policy, as different approaches could be taken to granular choice for the PHR and for the EHR.

With either approach, the issue of who is legally responsible for the data is a topic for consideration.

3. Large multi-patient, multi-entity data analyses.

The PCAST report contemplates the widespread use of health data for outcomes research, quality assurance, public health, effectiveness research, post-market device surveillance, and many other similar purposes. The impact on clinical care as well as the impact on multi-patient analyses of an architecture that uses data for multiple purposes needs to be investigated. Similarly, it should be determined whether the use of data for multiple purposes conflicts with other key policy interests, including privacy and consent. Technical and policy questions need to be explored regarding the use and transmission of de-identified data. The efficacy of the new exchange architecture for analytical work also needs to be determined.

A foundational issue is to identify and prioritize the clinical and analytical goals of health information exchange.

This issue has structural implications for the exchange architecture. A lower prioritization of "secondary uses" of data could impact the extent that information is exchanged at an atomic level, the use of provenance metadata, and the structure of indexes and directories.

4. Record Locator Services

a. Access. Policies need to be created to determine who is authorized to access the NWHIN through the record locator services (DEAS). Role based access rules need to be addressed.

b. DEAS Organizational Structure. The organizational structure and the financial model for the record locator services need to be determined. There are many options, including:

(1) Government entities, like the new insurance exchanges, or public health agencies.

(2) Business associates, like HIE organizations

(3) Covered entities, like health systems, or Accountable Care Organizations.

(4) Entities that may represent combinations of (1) through (3), like VA, DoD, IHS, state healthcare facilities, and local government healthcare facilities.

In addition to impacting the financing arrangements, the organizational structure of the record locator services (DEAS) has implications on the way governance is handled.

c. The record locator services (DEAS) will have data on an extremely large number of patients. The large quantity may create a need to consider new approaches to patient identification and matching processes.

5. Overexposure of Patient Information

Querying the record locator services (DEAS) may expose "false positive" information, such as in cases of human error, or when two patients share similar identifying characteristics, or when similar metadata tags exist. Policies need to be created that address under what circumstances a patient should be notified when his or her data or metadata are over-exposed through a search. Polices should also address the role of data holders in reducing the possibility of overexposure.

6. Quantity of Metadata

The large quantity of metadata that is concentrated in the DEAS is a distinctive aspect of the new exchange architecture. This large quantity of metadata may raise special privacy and security issues. For example, special security policies might be appropriate for the DEAS. Also, policies related to employees of the DEAS might be examined.

Alternatively, architectures that provide the same functionality without a concentration of metadata might be considered.

7. Governance

There are many governance questions related to the record locator services and to the end-state vision described in the PCAST report. For example: Who is responsible for the administration of DEAS and the enforcement of rules for DEAS? To what extent should governance be strong and centralized? What should the rules for DEAS include? What is the accountability mechanism? How do we assure data quality? How do we assure metadata quality? Will data mining of searches (accesses to DEAS) be monitored?

This governance issue is critically important to the success of the NWHIN.

8. Data holder autonomy, responsibilities, and liability

The proposed record locator services raise issues regarding the autonomy and liability of data holders, especially if DEAS users have automatic access to data in response to their queries. Providers and institutions may not be comfortable automatically sharing data with unknown or distrusted users, particularly where the access is brokered solely by authentication, role assignment and patient consent. Polices should address 1) The level of autonomy data holders maintain over how they share patient data under their control, 2) Liabilities data holders may incur from sharing data through the DEAS, 3) What tools and responsibilities data holders should have to ensure patient data is shared to legitimate parties for legitimate purposes, and 4) What responsibilities do EHR holders have to maintain a high level of accessibility to their data.

In addition, the PCAST vision creates several legal questions about the medical record. These questions include: How do the roles and responsibilities of a provider relate to data they create versus data they were sent, either from a patient's PHR or from another provider? What should the data creator be required to keep "in office" as we possibly move away from a document based construct? What do we now legally define as a "patient record"? Is there an impact on medical malpractice liability of using (or not using) NWHIN? Is there liability associated with transforming data through the exchange process (e.g., changing vocabulary or changing metadata)?

The workgroup makes the observation that provider participation in HITECH is voluntary. As a result, the way that liability questions are answered and the responsibilities of data holders may impact the rate of adoption of EHRs and NWHIN.

9. Education Programs and Transparency.

Both patients and providers need to understand the operations of the new exchange architecture in the context of an increasingly complex HIT environment. Transparency policies and educational programs will be impacted. It needs to be determined who is responsible for educating patients and clinicians about the PCAST exchange architecture and consequent privacy options. The effectiveness of various educational approaches needs to be examined. This issue has implications for the ability of patients to make meaningful choices. It may also impact the rate of adoption, if providers do not understand HIT operations. This topic has implications for ONC's REC program.

10. Metadata Regulation

The proposed new architecture raises a number of policy questions regarding the status of metadata tags, including the metadata tags that describe privacy preferences. These questions include:

a. Do the rules concerning data corrections also apply to metadata? For example, can patients make requests for corrections to metadata tags in the same way that they can request corrections to data?

b. Who is authorized to make metadata changes? Are there any special rules for changing provenance metadata?

c. Are the metadata tags subject to the same rules as data concerning audit trails and accounting for disclosures? If so, do metadata audit trails need to be propagated with the metadata?

d. If a patient changes or revokes a privacy preference that is described in metadata, how is that change propagated through NWHIN? To the extent that copies have been made of data elements, how are holders of the copy of the data element informed of the change? Is there an audit trail of changes to privacy tags? Is there an audit trail that lists instances where access was denied as a result of a privacy tag?

e. What are the privacy implications of using metadata generally and, specifically when aggregated within the DEAS? What levels of privacy protections should be given to the various types of metadata? Are there restrictions on how metadata may be used / disclosed?

11. Clinical Decision Making

The DEAS concept would enable a provider to search for, locate, and import clinical data about a patient and then to retrieve those data to assist in clinical decision making. The data would be retrieved in encrypted form, and could be decrypted only after the provider retrieved the encryption key from the DEAS. Once the provider viewed the data, the key would be destroyed, and the data would be either deleted or retained in encrypted form – to be viewed later only by again retrieving the key from the DEAS. Once a clinician has viewed clinical information about a patient, that information becomes part of the evidentiary basis for decisions the clinician makes with respect to that patient. As such, the retrieved data elements necessarily will need to be conveniently accessible in identical form, and with the same metadata tagging as they appeared at the time they were used in decision making. New policy and strategy will be needed around the DEAS concept as it applies to the retrieval, use, and retention of patient data to support clinical decision making.

COMMENT

This list of policies and questions should not be viewed as a complete list. As implementations proceed, and as policies are reviewed, many more topics will likely be raised.

Appendix D - Technical Architectural Concepts

The new exchange architecture includes the following directional **components and concepts**:

1. Use of an extensible language, with XML as an example.
2. A more atomic approach to exchange, using tagged data elements.
3. Record Locator / Data Element Access Service (DEAS) functionality
4. Persistent privacy safeguards that travel with the data
5. Decouple syntax and semantics, mapping controlled terminologies to the universal exchange language to support both semantic interpretation and varying levels of data specificity
6. Decouple security key management, data, indexing and aggregation.

PCAST HIT Report Technical Summary

We provide a summary of the technology proposed in the report, overview some of its key requirements with respect to scalability, security, and privacy, and speculate on a few of the gaps between existing capabilities and the proposed capability. The proposed technology, which we henceforth reference as the *new exchange architecture* is specified at a high level in the report itself and in presentations by the PCAST subcommittee in various forums, including their presentation at the FAC public hearings. Many details would need to be worked out to provide a complete specification; the explanation here is at the general level of the report but with some added comments on additional details required for implementation.

Proposed Functionality and Technical Architecture

The new exchange architecture aims to provide a search capability for medical records across institutions at a national scale, while providing strong privacy protections based on patient consent. The following diagram illustrates the primary components of the approach and an abstract representation of services that shift data between providers and users.

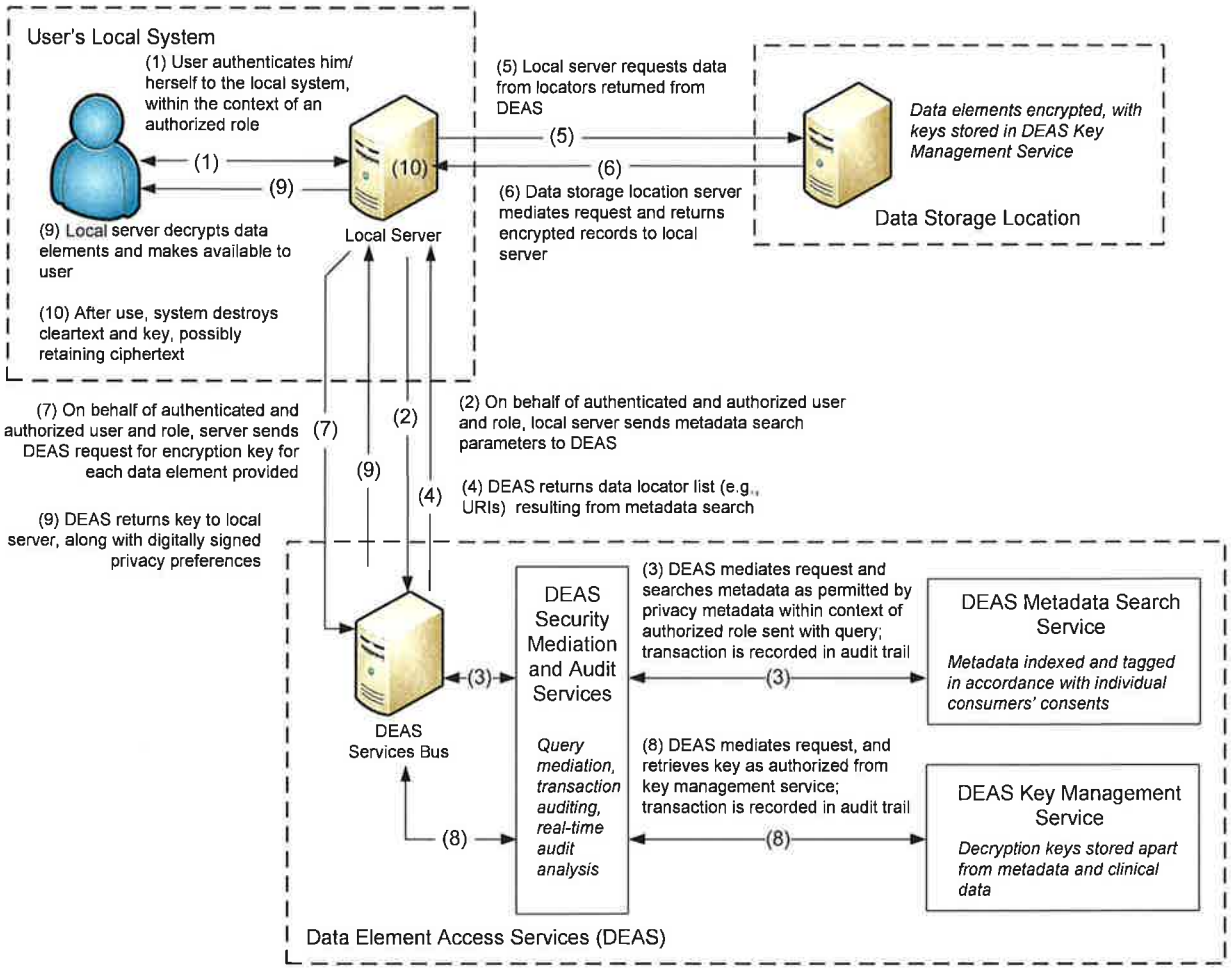
In this architecture, data providers such as hospitals and clinics supply health data in a standardized envelope called the Universal Exchange Language (UEL). The health data itself may be contained in a UEL record or referenced by it. Although the envelope will require a national standard, the health data contents could be in any of a variety of new or existing formats. The UEL comprises three primary components: (1) a *locator*, which provides a unique name and a way to find the data, (2) a *metadata* tag,

which provides key information about data contents, privacy, and provenance, and (3) the health data itself. This UEL data is accessed by data users though an interface called the Data Element Access Service (DEAS) which acts like a search engine on UEL data. In addition to its search function, which would involve an indexing system, the DEAS enforces policy by managing keys used to encrypt health data so that only authorized parties can read it and a global real time audit capability to detect abuses. Data providers and users will not be disjoint groups. Access to the DEAS itself would be limited, but should support at least two use cases: (1) a doctor can obtain records for a patient he or she is treating, with the consent of the patient, and (2) certain types of de-identified UEL data can be retrieved with the DEAS to assist research or public health functions.

Scalability, Security, and Privacy Considerations

Scalability of the new exchange architecture is a key element of its design. A point repeatedly made by the report and presentations of the PCAST subcommittee concerned the increased capability of current systems to perform such tasks as storage, high-speed delivery, and large-scale search. The architecture leaves considerable leeway about how to achieve sufficient scale. For instance, data does not need to be centralized, it could remain on storage of the provider that created it, but centralization in varying degrees is technically feasible, so that hosting services could provide efficient and inexpensive storage and delivery. The DEAS could be centralized (current search engines have shown capacity for enormous scale) or the overall service could be provided by a family of service systems.

Security of the system is essential. Protections rely significantly on a separation of duties wherein the DEAS does not directly handle medical data. The mechanism to achieve this separation is to insist that medical data is kept encrypted while it is not in use and that it is not accessed by the DEAS, which instead has access only to certain metadata. The following schematic shows the protocol.



A local user such as a doctor would query the DEAS through his or her local system. The DEAS would apply the query to its index of metadata and return a list of locators and descriptions (as search engines for the Internet and corporations work today). The local user would then select locators that are wanted and use them to obtain the wanted data, but only in an encrypted form. To see the data the local user needs to invoke the DEAS again to obtain the necessary keys for decryption. Note that the DEAS never retrieves the medical data and that the local user cannot view the data until he or she has obtained permission and keys from the DEAS. This authority enables the DEAS to keep a global record of access to records while it does not retrieve the health data itself. Other important security considerations include the inclusion of provenance information in the form of a digital signature on the UEL data, indicating, for instance, the provider that created it, and the need for authentication and authorization for access to the DEAS itself. A serious issue is the amount of sensitive information revealed to the DEAS by the meta-data alone. For example, meta-data indicating that there are results from an HIV test is potentially sensitive even if the results of the test are not revealed to the DEAS.

Privacy protections are perhaps the foremost design requirement of the new exchange architecture. The primary mechanism is to provide a privacy label as a metadata tag. This label would indicate allowed uses of the data and would remain attached to the data as it is passed to users as part of a search. The DEAS would use the label in authorizing access to keys to decrypt data and thereby assist in

persistent enforcement of privacy rules. The labels themselves could be specified by the patient, specified by the patient and provider, or specified as a service for the patient by an agent of the patient. Patients might choose not to have their data available to the DEAS at all. The report mentions the concept of making the UEL data packages as atomic as possible so that retrieved data can be more effectively managed on a need-to-know basis. For example, it should be possible to retrieve immunization records without retrieving mental health notes.

Gap Analysis

Scenarios for the DEAS and UEL sketched in the PCAST report are beyond the current state of the art for health information exchange at the national level. However, many of the technologies needed to accomplish it have been developed and deployed in other sectors. The FAC presentation of the report mentioned at least the following as evidence of feasibility: web technologies like HTML, XML, RDS, OWL; capabilities for search on the Internet and corporate networks; Digital Rights Management (DRM) systems for describing allowed uses of music and video; cloud storage and processing systems; data warehouses; large scale data mining and machine learning systems; broadband connectivity; and widespread low-cost computing devices. Moreover, some search and indexing systems have been explored in specific contexts like health registry systems and health information organizations so there is hope that emerging capabilities could be elevated to large scale and universal deployment. However, some aspects of the new exchange architecture are relatively novel and would require at least standardization, if not new designs. Some key examples include: (1) the ability to use middleware to take existing record systems and convert them to more atomic UEL data elements, (2) defining types of privacy protections that could be represented in metadata tags and finding a practical way to configure the protections that respects patient consent and other needs like public health, (3) developing an index system that does not place too much information in the hands of the DEAS and its users, (4) assuring that the key management system of the DEAS is scalable for use in an inter-domain context, and (5) developing suitable distributed architecture and governance for the DEAS.

Appendix E—Implementation Task Force Report

The Taskforce was asked to develop two or more illustrative examples of Implementation Approaches to achieve the directions and vision of the PCAST report. These examples were to clarify what was meant by an Implementation Approach", i.e. how the different components of an approach work together, and to bring out the common aspects of different approaches. Dixie Baker, Carl Gunter, John Halamka, Stan Huff, Wes Rishel, and William Stead participated in the Taskforce.

The Taskforce developed three Use Cases which correspond to three Levels of Exchange supported by a UEL and DEAS. We'll call them "push by patient of data between two points," "simple search for data," and "complex search for data." They are intended to support PHR and EHR health information exchanges for a multitude of uses, include clinical care, population health and clinical research. A fourth Use Case incorporates de-identified data.

Use Case 1 - Push by patient between two points:

The patient logs into a tethered PHR via username/password or other authentication mechanism provided by the clinical organization hosting the data. The patient chooses to push the data to the non-tethered PHR of their choice. Many possible architectures and approaches can support this including download from the tethered PHR with upload to the un-tethered PHR, a push directly from the tethered PHR to the un-tethered PHR (as Google Health and Microsoft Health support today), or the use of secure email from the tethered PHR to the un-tethered PHR using the Direct standards via a secure health email address. In each case, the data sent wrapped in a UEL envelope containing patient identity, provenance, and privacy metadata information. UEL Metadata might also include non-disclosing information about the categories health data available in the content package i.e. medication list, problem list, allergy list, labs, radiology images etc.

When the UEL arrives at the non-tethered EHR, data is shown to the patient, who can elect to incorporate structured and unstructured data into their existing un-tethered PHR dataset. Then, the patient can then choose to share PHR data with clinicians, clinical researchers, or public health by pushing selective PHR data wrapped in an UEL envelope via secure transmission (such as Direct) to recipients of their choice. Organizational certificates are needed for the senders (un-tethered PHR hosting organization) and the recipients (clinician offices, clinical research organizations, public health organizations). Audit trails are held by senders, recipients and any Health Information Service Providers used as part of Direct transport. Patient authentication is username/password as required by the PHRs. Provider authentication is username/password or other modality as required by the EHR.

Summarizing the infrastructure for this approach, we will need
*A UEL that includes patient identity, provenance, privacy metadata, and categories of health data

available in the content package. There will need to be semantic standards for this metadata including the content/vocabulary of identity, providence, privacy metadata, and categories of health data.
*Applications which are capable of wrapping content packages of clinical data in the UEL
*Applications which are capable of receiving the UEL and unwrapping content packages
*Certificate management to secure the endpoints and support privacy controls
*Policies that support push of data between two points.

Use Case 2 - Simple Search:

A patient presents to an Emergency Department and notes that his records are stored at a specific clinician office and a specific hospital. If necessary, an Emergency Physician obtains patient consent to retrieve his records. A query is created that includes patient identity, consent information, and provider authentication data. A Data Element Access Service which serves as an entity level provider directory is securely queried to determine the Uniform Resource Identifiers (URIs) of the clinician office and hospital. The query is sent to the URIs, which return a UEL wrapper containing identity information, provenance, patient privacy metadata based on any consents on file at the organizations hosting patient records, and non-disclosing information about the categories health data available in the content package. The content package inside the UEL includes numerous appropriate vocabularies. The receiving clinician can choose to incorporate structured and unstructured data into the Emergency Department record. All exchanges are query/response. Organizational certificates are needed for the Emergency Department, the clinician office and the hospital. Audit trails are held by all these organizations. Provider authentication is username/password or other modality as required by the ED information system or national policy.

Summarizing the infrastructure for this approach, in addition to the infrastructure of Use Case 1, we will need:
*Policy for issuing queries to organizations hosting patient records
*A DEAS that includes entity level provider directory information to provide the URIs of provider data sources
*The syntax and semantics of a query for clinical data including identity information that is sent to provider organizations hosting patient information
*Applications which are capable of issuing a query to known URIs
*An approach to disambiguate identity conflicts if the query results in multiple patient matches

Use Case 3 - Complex Search:

A patient presents to an Emergency Department and is non-responsive. However, her wallet contains an ID with name and date of birth. An Emergency Physician, based on policy which grants implied consent for unconscious patients, clicks the external search icon in their EHR. The EHR creates a query containing patient identity, implied consent information, and provider authentication and role, then sends it to a Data Element Access Service. The DEAS returns a list of Uniform Resource Identifiers of the

organizations which hold the patient's records. The Emergency Physician's EHR sends a query containing patient identity, consent information, provider authentication and role to each of the URIs, with a request for problems, medications or allergies. Each organization returns as many UEL wrapped data packages as match the query and pass the conditions of patient privacy metadata based on any consents they have on file. Each UEL wrapped package includes identity, provenance and privacy metadata and non-disclosing information about the categories health data available in the content package. The content package inside the UELs includes numerous appropriate vocabularies. The receiving EHR filters and organizes the information for the clinician who can choose to incorporate structured and unstructured data into the local Emergency Department record. All exchanges are query/response. Organizational certificates are needed for the Emergency Department, the DEAS provider, and the organizations which contain patient records. Audit trails are held by all these organizations. Provider authentication is username/password or other modality as required by the ED information system or national policy.

Summarizing the infrastructure for this approach, in addition to the infrastructure of Use Case 2, we will need:
*Policy for issuing a query to the DEAS
*A DEAS which contains patient identity information, provider URIs and potentially more granular information about the types of data available at those URIs
*The syntax and semantics of a query including identity information that is sent to the DEAS.
*Applications which are capable of querying a DEAS and then querying URIs of provider data sources specified by the DEAS, assembling the data returned into a meaningful display
*Support for privacy metadata that are returned by the DEAS and provider data sources

Interoperation among Use Cases 1-3:

The Use Cases and the Levels of Exchange are not mutually exclusive. If all three are supported, the patient in Use Case 1 can use the simple search of Use Case 2 to query for the URI of a provider they would like to push their information to; and the complex search of Use Case 3 to expose a UEL wrapped subset of their PHR to the DEAS tagged with a privacy tag indicating their desire that it be made available to someone giving them care and a provenance tag indicating that she had edited it.

Use Case 4 - De-identified aggregate data search and retrieval

A researcher wants to retrieve de-identified mammograms to investigate a new technology that provides computer assisted interpretation. This is a use for which it is not necessary to describe the population of women from whom the mammograms were obtained, or to have detailed information about the women or their medical history. The researcher issues a query to the DEAS requesting de-identified mammograms that are reusable for research based on patient consent. A list of URIs is returned including pointers to mammograms. The researcher queries the URIs and receives de-identified mammograms.

Summarizing the infrastructure for this approach:
*Policy for issuing a research queries to the DEAS
*A DEAS which supports de-identified queries for a specific type of data
*The syntax and semantics of a query including data type information that is sent to the DEAS.
*Provider data sources that are capable of returning de-identified data
*An application that can query a DEAS and query provider data sources
*Support for privacy metadata that include consents (where required by law or policy to release data for research and ensure de-identification)

Implementation Table:

The Taskforce identified 15 components or capabilities that work together to make up an Implementation Approach. The first is the end user, i.e. what the actual person needs to do. Next is the local system, i.e. what their local EHR needs to do. The Taskforce defined the UEL as a language (syntax) that captures the logical structure of clinical data and the binding of the coded elements in the structure to standard coded terminologies and or ontologies. The Taskforce identified 4 components of an Implementation Approach related to the UEL: 1) its syntax, i.e., the structure; 2) the required metadata, i.e. the semantic standards for privacy, provenance, and identity metadata; 3) a naming authority, i.e. a service to manage the naming and versioning of the UEL syntax, the metadata semantics, the clinical data structures such as the CCD and clinical data semantics; and 4) the mechanism of the binding coded element to standards. The Taskforce developed the schematic of a full function DEAS that is included in Appendix D. It shows that each query response would involve ten steps. For the purposes of the Implementation Table, the Taskforce simplified the components related to the index/search as: 1) what the index/search service needs to do; 2) what the sources that hold data would have to do to respond to the service; 3) the privacy implications of the above interactions; and 4) the aspects of the query language that would be necessary. The other components that make up an Implementation Approach are the mechanism for achieving separation of duties; audit; authentication for both patients and providers; and the policy implications of the Implementation Approach.

The components or capabilities are represented as rows in the implementation table. The component's name is in the left column of the table. The Taskforce created columns in the table for an Implementation Approach matching each of the three use cases. In this way, cells to the right show of the component name show what that component needs to be able to do to support each of the use cases.

The table shows that the three implementation approaches are actually three levels of progressive support for information exchange. In the first level, all exchange would be done within the context of a PHR and in the context of our existing policies. In the second level, the search would need to be able to locate known sources, adding the requirement of a DEAS capability. It would be an extremely thin DEAS because all it would need to do is find the location of the person holding the record. None-the-less table shows new policy and governance would be needed as would a capability to disambiguate identity. The third level, represents the Taskforce's understanding of the PCAST end state. It would require full definition of each of the components and all the related policies.

Components	**Level 1 (UC1) – Push by patient**	**Level 2 (UC2) – simple search**	**Level 3 (UC3 + more clinical query of DEAS) – complex search**
End user	Provides consent preferences to provider Logs into tethered PHR and retrieves encrypted and digitally signed record wrapped in UEL Pushes wrapped record to untethered PHR Logs into untethered PHR and sets privacy preferences	Asks patient for sources where health information may exist Logs into system under authorized identity and role Uses system to find record location and to request/receive data	Uses system to query DEAS and to request/retrieve data
Local system	Encrypts and digitally signs record made available to patient through tethered PHR	Resolves identity conflicts Queries directory for location Uses Direct to encrypt, digitally sign, and transmit request for record location, along with authenticated identity and role of requester Receives UEL from	Acting on behalf of authorized user and role, sends query to DEAS in UEL wrapper Receives locators from DEAS Acting on behalf of authorized user and role, sends data request to record location Receives encrypted,

Components	Level 1 (UC1) – Push by patient	Level 2 (UC2) – simple search	Level 3 (UC3 + more clinical query of DEAS) – complex search
		record holder(s) Unwraps received UEL, validates digital signature of source, decrypts data, and makes available to end user within meaningful context	digitally signed record Validates digital signature of sender Acting on behalf of authorized user and role, sends to DEAS a request for encryption key for each data element received Decrypts encryption key provided by DEAS, decrypts data, and makes available to end user within meaningful context
UEL – syntax, including versions of the syntax	Outer wrapper for transport Inner structure for 3 metadata blocks (identity, provenance, privacy) & 1 clinical data block (clinical metadata is in the clinical block)		Inner structure for a 4th metadata block (clinical) Each block is encrypted using a unique encryption key, and digitally signed
UEL – required metadata	Semantic standards for provenance, privacy	Add semantic standards for identity metadata	Add semantic standards for clinical metadata
UEL – naming authority for terminologies, name spaces and versions	Manages naming and versioning for: UEL syntax Metadata semantics	Add identity metadata semantics	Add clinical metadata semantics

Components	Level 1 (UC1) – Push by patient	Level 2 (UC2) – simple search	Level 3 (UC3 + more clinical query of DEAS) – complex search
	(provenance, privacy) Clinical data structures, CCD etc Clinical data semantics		
UEL – binding of coded elements in the model to terminologies, name spaces, and versions			
Index/search - service	(all exchange would be done within PHR)	Locate known sources	Locate requested clinical data types, for an identity, subject to privacy preferences and role Key management
Index/search - sources	Couple to PHRs & external EHRs etc Transmit data in UEL	Provide information about an identity	Provide requested clinical data types, for an identity, subject to privacy preferences and role
Index/search – privacy implications	There is no index or seach with this use case.	Patient consents to have provider request and receive health information from named record location	Patient consents to have information indexed in DEAS Patient establishes granular consents for indexing (based on data type, provider, role, context, etc.) DEAS protects data in accordance with laws and regulations, as well as patient consents

Components	Level 1 (UC1) – Push by patient	Level 2 (UC2) – simple search	Level 3 (UC3 + more clinical query of DEAS) – complex search
			Each data element is separately encrypted using symmetric encryption, with key escrowed within the DEAS key management service DEAS search service contains only metadata; clinical data are retained by their sources To obtain clinical data requires separate actions to 1) search metadata in DEAS, 2) retrieve clinical data from source, and 3) retrieve encryption key from DEAS.
Index/search – query language	At discretion of untethered PHR vendor.	Requests wrapped in UEL along with authorized identity and role of requester Need for standard terminology for requests	Metadata are published to DEAS, which indexes metadata for search Search parameters sent in UEL
Separation of duties	Local system responsible for making clinical data available to patient in accordance with HIPAA and local policies Patient responsible for logging into tethered	Patient's provider responsible for requesting and receiving data in accordance with local policies and patient preferences	(see Index/Search – privacy implications above)

Components	Level 1 (UC1) – Push by patient	Level 2 (UC2) – simple search	Level 3 (UC3 + more clinical query of DEAS) – complex search
	PHR and for pushing data to untethered PHR of her choice Untethered PHR vendor responsible for managing security of Internet PHRs.	Record location responsible for receiving request and sending data in accordance with local policies and patient preferences Provider directory includes only location information, no patient information	
Audit	Actions within provider systems (EHR and tethered PHR) are audited i.a.w. HIPAA; audit record is available to patient Auditing of actions within untethered PHR is at the discretion of the PHR service provider	Actions within provider's systems are audited i.a.w. HIPAA; audit record is available to patient	Actions within provider's systems are audited i.a.w. HIPAA Actions within DEAS are audited Audit records are available to patients
Patient authentication	Patients are authenticated to tethered PHR in accordance with provider's policy Patients are authenticated to untethered PHR in accordance with service provider's policies	N/A	N/A
Provider authentication	Providers are authenticated to local system in accordance	Providers are authenticated to local system within	Providers are authenticated to local system within

Components	Level 1 (UC1) – Push by patient	Level 2 (UC2) – simple search	Level 3 (UC3 + more clinical query of DEAS) – complex search
	with local policies	authorized role Requests to record locations include authenticated identity and role of requester	authorized role Requests to DEAS and to record locations include authenticated identity and role of requester
Policy implications	Provider systems governed by HIPAA privacy and security rules Untethered PHR governed by FTC regulations Policies relating to treatment and protection of metadata	Current policies	Need policies around the indexing of patient records within the DEAS, and enforcement of patient and institutional privacy rules Need to determine DEAS status w.r.t. current HIPAA rules

Definition of UEL – a language (syntax) that captures the logical structure of clinical data and the binding of the coded elements in the structure to standard coded terminologies and or ontologies.

Definition of atomic – smallest meaningful piece of information about a patient.

APPENDIX F—Deployment Models

Middle-Out Activities

The following list of activities was suggested by some members of the workgroup for the Middle-Out Deployment Model:

a. Data: Establish naming standards, and expand vocabulary efforts. Identify standards for the"data abstraction layer", which is the de-normalized data that might be represented with middleware.

b.Metadata: Identify standards for metadata. Standards may include naming standards.

c. Privacy Preference: Establish standards and/or rules that reflect laws and privacy policies and enable patients to dynamically assert privacy preferences where applicable.

d.UEL: Specify the UEL syntax standards and other related standards, including the components listed in Appendix E.

e.Access Tools: Identify standards for tools that access data through the DEAS. Identify language or other standards for performing data analyses.

f. Infrastructure: Identify standards for necessary information exchange components (e.g. security and communications standards)

h. Coordinate activities with the resolution of the policy issues that are raised.

The following table compares the three deployment approaches.

Accomplishment	Top-Down	Bottom-Up	Middle-Out
Resolve Policy Questions	Necessary precursor, broadest range of policies	Necessary precursor, perhaps not as comprehensive as Top-down	Necessary precursor, perhaps not as comprehensive as Top-down

Accomplishment	Top-Down	Bottom-Up	Middle-Out
Define IFaP standards and operational requirements for 15 components	Fully specified to the level of certification and meaningful use	Industry players collaborate to establish the extent to which standards are needed; multiple, non-interoperable approaches may arise	ONC establishes minimal IFaP for initial goals; encourages industry to add IFaPs above the minimum set.
Establish governance body	Precursor: governance for all capabilities of DEAS	Minimum necessary to enable the trust necessary under HIPAA, more likely as determined by resolution of policy questions	Minimum necessary to support any meaningful use case used as an incentive.
Create operators of DEAS services	Government funded	Industry	Location service may be government funded
Incentives	Contracts from large Federal agencies that deliver care or pay for care that require the specified standards.	SBIR; funds to assist the development of open source communities.	Contracts from large Federal agencies that deliver care or pay for care that require the specified standards.
EHRs meaningful use incentives require certification regulation and meaningful use measures	All necessary standards for sources and users of data; appropriate MU measures	Deferred until concept is proven technologically and economically	Initially based on building block standards.