**Comments of Patient Command, Inc.**
**In response to**
***Reboot:***
***Re-Examining the Strategies Needed to***
***Successfully Adopt Health IT***
**April 16, 2013**
**Senators Lamar Alexander, Richard Burr, Tom Coburn**
**Mike Enzi, Pat Roberts, John Thune**

Submitted May 13, 2013

**Table of Contents**

**Executive Summary**

The federal government has failed to develop a technically feasible network design for nationwide exchange of health records and other health data among patients, doctors, hospitals, pharmacies, insurance companies and other payors, and others who would participate in routine exchange of health data. *Reboot* accurately, and with some restraint, recites the inability of the Office of the National Coordinator for Health Information Technology (ONC) to carry out its mandate under the HITECH Act, part of the American Recovery and Reinvestment Act of 2009.

This document responds to *Reboot*'s invitation to participate in a dialog about ONC's inability to make progress under HITECH. We believe ONC under two administrations has pursued the wrong architecture for nationwide health information exchange.

Were ONC to concentrate instead on integrating health records around patients, society would realize great benefits. If patients had easy, affordable access to compilations of their own aggregated records, they would make more informed, better decisions in the marketplace. The healthcare services market would become more efficient; societal costs for healthcare would decrease. This is essential to reining in health system costs, and key to better health outcomes.

ONC has long tried to achieve interoperability among institutional Electronic Health Record (EHR) systems operated by physicians, hospitals, and other providers. The EHR systems would use a network allowing, for example, a given doctor to request all other EHR systems on the network to identify whether they held records for a particular patient and, if so, to transmit those records to the requesting doctor. There the various providers' records would be assembled by the treating physician's EHR system and used to diagnose or treat the patient.

We explain why that systems design, "provider-query," has proved technically unattainable. It cannot be successfully engineered using currently available technology.

We also analyze how ONC has failed to develop interoperability standards, which are the essential foundation for accomplishing all subsequent tasks under HITECH. ONC has failed to follow HITECH's structure because it is pursuing "Meaningful Use" of interoperable technology before the protocols for interoperability are developed and promulgated. This mistake has doomed ONC's efforts under the statute. ONC's serial failures, now more widely apparent, have prompted *Reboot.*

Yet there is reason for optimism, because an alternative network design is readily attainable. It is based on interconnecting patient records compiled from various providers and stored securely in repository (health record bank) accounts that patients own, and access to which they control. Integrating health records around patients using an existing format (the "Continuity of Care Document," or CCD) and connecting them via a network message standard protocol already acceptable to ONC, "Direct," is within reach now.

We also offer a brief introduction to how identity management and authentication issues can be addressed in the network design framework we propose. We conclude by suggesting criteria Congress can use in bipartisan planning of how best to achieve the goal of nationwide health data exchange.

## 1. Introduction – Achieving Health Data Exchange Through a Workable IT Architecture

Since 2001 Patient Command, Inc. of McLean, Virginia, has been developing a system for patients to collect, compile, control access to, exchange, and otherwise use their health information to help manage their health and health care. We are pleased to offer these observations in response to the invitation from the senators who authored "*Reboot.*"

We agree with *Reboot's* authors that policies and programs adopted by the Office of the National Coordinator for Health Information Technology (ONC) have failed to meet the promise envisioned in HITECH.[1] That vision is of a secure nationwide system for sharing health records in digital form. We offer a brief analysis of how ONC, almost from the start, chose an unworkable system architecture to implement HITECH. ONC remains on that wrong course today.

ONC's choice for health data exchange is what we will call a "*provider-query-based network architecture.*"[2] Experience during the administrations of President George W. Bush and President Barack Obama repeatedly proves this architecture will not work at scale.[3] Available technology cannot support it, as we explain below.

---

[1] Title XIII of The American Recovery and Reinvestment Act of 2009, Pub. L. 111-5 (the "HITECH Act").

[2] ONC acknowledges that its choice of provider-query-based network architecture cannot succeed in achieving nationwide health data exchange. Department of Health and Human Services, Office of the Secretary, Centers for Medicare & Medicaid Services, *Advancing Interoperability and Health Information Exchange*, 78 Fed. Reg.14793, 94 (Notice and Request for Information, March 7, 2013) :

> The Medicare and Medicaid Electronic Health Record (EHR) Incentive Programs and Office of the National Coordinator (ONC) for Health IT (HIT) Certification Program are increasing standards based health information exchange (HIE) across health care providers and settings of care to support greater coordination of health care services. *However, this alone will not be enough to achieve the widespread interoperability and electronic exchange of information necessary for delivery reform where information will routinely follow the patient regardless of where they receive care.*

*Id.* (emphasis supplied).

[3] *See generally,* W. Rishel, et al. (Gartner, Inc.), *Summary of the NHIN Prototype Architecture Contracts*, Report for the Office of the National Coordinator for Health IT, May 31, 2007, available at http://www.healthit.gov/sites/default/files/summary-report-on-nhin-prototype-architectures-1.pdf. This pre-HITECH report should be read, not so much for its analysis and laudatory conclusions, but for what it missed. The report summarizes four substantial projects exploring architecture for the proposed national health record exchange network. The four contractors were Accenture, CSC, IBM, and Northrop Grumman. The report praises the four projects for exploring complexity in health data exchange and for drawing conclusions about what a national "network of networks" would look like. Those networks would use variations of what we are calling here a provider-query-based architecture. Six years later, readers will observe that the four prototype projects have not served as the basis for ONC's (or anyone else's) engineering a successful health data exchange network, whether on a local, regional, or national

An architecture that is scalable nationwide[4] is within reach, however, and we propose that Congress evaluate it.[5] This architecture offers a pragmatic approach, using available technology, for achieving HITECH's goals and other objectives such as routinely, affordably, and securely exchanging the health records of military members and veterans.

The architecture is based on using secure repositories offering consumer-controlled data accounts. There patients can accumulate, compile, review, analyze, send, and grant access to their health records to providers, family members, advisors, researchers, and others. The repositories, called "health record banks," would be connected by a secure backbone. The

---

scale. With hindsight and six years' experience, we know these four projects demonstrate instead the insurmountable technical complexity of scaling up any system based on provider-query architecture, and hence the engineering infeasibility, of any health data exchange based on a provider-query template and constrained, as are all health network designs, by the limitations of currently available technology.

[4] V. Lapsia, K. Lamb, W. Yasnoff, *Where should electronic records for patients be stored?*, 81 Int'l. J. Medical Informatics 821 (2012) (simulation studies show that the "distributed" (provider-query) architecture – where each patient's records are likely to be spread over multiple nodes – is greatly inferior to the "patient-centric" (patient record repository account or health record bank) model in terms of transaction efficiency (it requires exponentially more transactions); scalability; data retrieval integrity, accuracy, and completeness (it inevitably produces substantially more errors); usability; and timely availability of access):

> In the distributed model multiple queries are needed to retrieve the fragmented patient data from the source nodes, whereas only a single query is required to obtain a patient's file in the centralized model. By design, large distributed systems with heterogeneous data sources incur a query performance penalty. Various methodologies and techniques that optimize the query performance and improve scalability and workload adaptability have been proposed and validated. An example of such optimization is the use of a 'Record Locator Service' (RLS) or similar index to identify and track the file locations of each patient's records. In the distributed model, a patient's record would be retrieved via queries to the various sites of care documented in the RLS at the time of previous encounters. Query search optimization using a solution such as an RLS dramatically reduces the cost of locating nodes with relevant data in a distributed model. *However, unlike the centralized model, the distributed model will still incur the cost of multiple queries to assemble the patient's record, in direct proportion to the extent of fragmentation.* Essentially, the total number of queries required to retrieve a single patient's complete record in the distributed model will at the very least equal the number of nodes across which the record is fragmented.

*Id*. at 822 (footnotes omitted, emphasis in original). This article explains why the provider-query model cannot be scaled up for a nationwide health information architecture.

[5] *See* W. Yasnoff, L. Sweeney, E.H. Shortliffe, *Putting Health IT on the Path to Success,* Vol. 309, No.10 *J. Am. Med. Assn.* 989 (March 2013)(recounting ONC's failing programs to support the provider-query model as essentially seeking "to replicate existing manual processes for contacting other clinicians or health care organizations to get patient records," listing the deficiencies of that approach, and pointing to health record banks as a better architectural foundation that is "simpler, scalable, less expensive and more secure," *id.* at 990).

backbone, or hub, would enable a "publish and subscribe" protocol using a variant of an interconnection protocol, "Direct," already under development and known to ONC.[6]

The virtues of this architecture are considerable. It is feasible and affordable. It also would introduce new market mechanisms for controlling health care costs by giving consumers information they need to make informed decisions when purchasing health care products and services. It would enable, but not require, consumers to "engage" by giving them easy, inexpensive, routine Internet access to their own health data, which they could study, analyze, and use for more efficient management of their health and health care. It would help patients invest in wellness in addition to spending to control or cure illness.

We turn to the centrality of patient engagement as a prime criterion in selecting a health data exchange architecture that can be scaled for a nationwide infrastructure.[7]

## 2. Refocusing Objectives of Digital Health Information Exchange – Integrating the Network Patients' Access to and Control Over Their Compiled Data to Alter Healthcare Market Behavior, Lower Costs, and Improve Care

Our starting point is with healthcare costs. Hopes for reducing the rapid escalation of healthcare costs are as important a goal of health IT as are improved patient care and better outcomes. Yet discussion of runaway costs often omits analyzing how our present system hinders patients in making rational decisions when purchasing care in the U.S. healthcare market. We hinder patients by largely excluding them, the consumers of care, from access to information (their own records) essential to their purchasing choices. Meanwhile, we make health records routinely available to many others, such as providers, insurers, vendors, and regulators.

One could hardly devise a more inefficient, essentially anti-market, mechanism. Is it any wonder that costs in the U.S. healthcare market increase rapidly and continually?

*Reboot* itself falls into this trap, no doubt because we as a society are in the habit of forgetting about the centrality of patients when discussing health IT. We focus on doctors and hospitals. Here is an example:

> 'Health information technology,' as referred to in federal law and in this white paper, broadly refers to electronic storage of records, electronic billing, electronic ordering of tests and procedures, and even a shared, interoperable network to allow *providers* to communicate with each other.[8]

The picture of health IT as an exchange mechanism primarily for providers, rather than as a system integrated around healthcare consumers (patients) and designed to help patients make

---

[6] For discussion of Direct, see *infra* notes 17 & 20 and accompanying text starting on p.12.

[7] The Appendix to these comments is a graphical comparison of "provider-query" architecture to the "patient-centered repository" or health record bank architecture. It illustrates why the provider-query model cannot be scaled to support a nationwide health information infrastructure.

[8] *Reboot* at 6 (emphasis added). Here is another example: "If *providers* are not able to achieve meaningful use of their new technologies, they will not be in a position to share electronic records with other *providers* at the interoperability stage." *Id.* at 13 (emphasis supplied).

sensible choices in cooperation with providers and other advisors, appears throughout *Reboot*. It is an ingrained assumption in analyses of U.S. healthcare.

Thus we have a market in which under-informed consumers are incented to buy health services, most often because they are sick and sometimes because they want to stay healthy. They usually have means to purchase almost unlimited expensive services because they are insured. Meanwhile, the sellers – doctors, hospitals, and other providers – are primed to sell more and more expensive services because most care is reimbursed under a business model from the 1960s (based on Medicaid and Medicare). This is a system primed to produce rising costs.

The practice of keeping important health information (the contents of their own medical records) from consumers helps to perpetuate this fundamentally inefficient health care market. Its underlying premise is that medical information is too arcane for untrained consumers to use when making healthcare choices, and hence when selecting healthcare services to purchase.

Today in the U.S. this premise is wrong. We have both technology to make people's medical records available to them privately and securely, and a range of advisors and advisory services to help them use that information in making sensible healthcare purchasing decisions. We could therefore create a far more efficient market for health services and products.

We can use this realization to reorient public policy for health information exchange by redefining our basic goal thus: *The purpose of health IT is to compile health information from various providers and other sources, and place that information in a secure repository under the patient's control so that the patient can make it available in whole or part at various points of care or for other purposes such as research in which the patient wants to participate.*

The re-orientation to a patient-centric model for health care information exchange leads directly to a corollary: The most efficient way to implement health information exchange is to establish secure repository accounts so that patients can deposit their health records in compilations they control, and to which they can grant access to providers, medical researchers, family and trusted advisors, insurers and others as appropriate. Access and information exchange is accomplished through secure networks. We deal below with some authentication and other privacy and security features that can be used for these networks.

The "engaged patient" is a goal of much writing about health IT policy. Patients who lack routine access to their own health records have difficulty maintaining the level of engagement necessary to manage their health effectively long term. Conversely, giving patients routine, easy, inexpensive, secure Internet access to their own health information is probably the best approach to engage them for the long run in helping to manage their health and healthcare.

Integrating health information around the patient-consumer to whom they pertain is inherently efficient. It can be the basis for a redesign of health information exchange under HITECH. It is a practical network architecture in contrast to the principal architecture that has been ONC's focus under HITECH, and to which we now turn.

### 3. Understanding ONC's Selection of an Unworkable Network Architecture for Health Information Exchange

When ONC first sought to implement HITECH, it set a course that disregarded both law and logic. ONC did so (prodded by the Policy Committee established under HITECH) because it sought to define "Meaningful Use" of "Certified EHR Technology" prematurely. ONC attempted to define "Meaningful Use" before establishing the interoperability standards that HITECH specifically requires as a prerequisite to any such definition.[9] The consequences of this mistake bedevil U.S. health IT programs to this day. This is the root cause of the deficiencies outlined in *Reboot.*

Subtitle A of HITECH, Section 3000, dense and prolix, is fundamental. Under subsection 3000(13)(B)(iv), a "Qualified Electronic Health Record" must include the capacity for what we understand colloquially as interoperability. Here is that subsection:

> [Qualified Electronic Health Record. – The term 'qualified electronic health record' means an electronic record of health-related information on [*sic*] an individual that –
>
> (B) has the capacity–
>
> (iv) to exchange electronic health information with, and integrate such information from [*sic*] other sources.

Earlier in Section 3000, in subsection (1), the term "qualified electronic health record" is used to define "Certified EHR Technology":

> The term "certified EHR technology" means a qualified electronic health record that is certified pursuant to section 3001(c)(5) as meeting standards adopted under section 3004 that are applicable to the type of record involved . . . .

ONC is charged in Sections 3001-3009 with overseeing the standards development process for Certified EHR Technology. Adopting these standards is crucial, because what is to be "used meaningfully" under HITECH is Certified EHR Technology. If the standards used to define how an EHR will "exchange electronic health information with, and integrate such information from other sources" (subsection 3000(13)(B)(iv)) are not established first, then any discussion of Meaningful Use becomes meaningless. How is any doctor or hospital to know how to use Certified EHR Technology meaningfully when the standards underlying the secure exchange of health data are left to some later time?

The quandaries summarized in *Reboot* are consequences of this fundamental mistake at ONC. For example, *Reboot* notes the proliferation of entities with overlapping, and perhaps conflicting, health IT roles:

> [H]ealth IT policy is governed by a complicated patchwork of overlapping federal legislation and standards. Federal laws and standards are implemented through CMS, the

[9] The areas for which the standards are required are listed in Section 3002(b)(2)(B) of HITECH. They include security, privacy, a nationwide technology infrastructure for the electronic use and accurate exchange of health information, and use of a certified EHR for each person in the United States by 2014.

> Office of the National Coordinator for Health IT, the Agency for Healthcare Research and Quality, the Health Resources and Services Administration, and the National Institute of Standards and Technology, among others. Additional entities working on standards include the Health Information Security and Privacy Collaboration, which is developing a national privacy and security framework, the Health Information Technology Standards Panel, a public-private effort to develop standards for the certification of health IT products, and the National eHealth Collaborative, a public-private advisory body to make recommendations on health IT adoption and usability. The multiplicity of actors and entities has created a confusing, complicated system of requirements that providers must navigate in order to avoid mandated penalties for noncompliance. These compliance burdens are largely not in sync and create a tangle of requirements that may be well intentioned, but will likely be opaque and confusing to stakeholders.[10]

These organizations and others in the private sector are foundering because they are, essentially, attempting to compensate for the basic, fatal structural weakness in ONC's Meaningful Use criteria. That structural flaw is the absence of data exchange standards for information to be sent back and forth among the vast array of disparate EHR systems already installed throughout the U.S. These disparate health record systems use different, proprietary code structures, operating systems, and communications protocols that make them incompatible and non-interoperable with most other installed EHRs bought from other vendors.

Omitting the essential first step of defining standards for a specified initial (and presumably rudimentary) level of health information exchange, ONC concentrated instead on trying to define Meaningful Use. Because Meaningful Use of interoperable data exchange cannot have real meaning until the initial specifications for the data exchange are defined in a government-adopted standard, ONC's approach has proved infeasible. (ONC did not perceive this infeasibility, nor did the ONC Policy Committee.) However, some in the health IT industry knew soon after HITECH's enactment, and after the first few meetings of the Policy Committee, that ONC's chosen course would fail.

*Reboot* correctly concludes that ONC's federal subsidies continue to make the problem worse week-by-week. ONC's programs encourage doctors and hospitals to install more of these incompatible systems, that is, systems that are non-interoperable under the criteria demanded in HITECH subsection 3000(13)(B)(iv). Of course, they are not interoperable because ONC did not publish interoperability (data exchange) specifications. ONC instead concentrated on fleshing out Meaningful Use, despite the obvious proposition that "Use" cannot be "Meaningful" until everyone knows how and the extent to which a federal government exchange standard will control health data exchange nationwide.

Here is the fundamental logical, engineering, and legal precept that Congress, HHS, and ONC should adopt in rebooting efforts to create a systems design that will actually work for nationwide health data exchange: *both in law and systems design logic, HITECH's core – and by far most difficult – task is developing standards for secure data exchange in health IT.* That task must come first. It is the foundation for everything else in HITECH. ONC unfortunately bypassed it.

[10] *Reboot* at 25.

Until Congress corrects that mistake and mandates adoption of that systems design approach, the foundation for further progress under HITECH does not exist. Congress must, through oversight or legislation, require ONC to develop and publish mandatory initial data exchange standards.

At present, therefore, it is idle to speculate about what doctors and hospitals should be required to do under Meaningful Use (though ONC's Policy Committee continues to do so in exquisite detail). It also is ultimately useless (and vulnerable to successful legal challenge) to incorporate the Policy Committee's Meaningful Use wish list into HHS regulations.

Any federal judge who reviews those regulations under the Administrative Procedure Act (which applies to ONC's implementation of HITECH) would readily see violations of law. Meaningful Use regulations that are not based on published federal interoperability standards, are by definition under HITECH, arbitrary and capricious.[11] That is an inevitable, unavoidable conclusion. Put another way, and incorporating systems engineering logic into the HITECH legal analysis: If no one knows what data must be exchanged because they do not know how it will be exchanged, and do not know what format or other requirements the data will have to meet in order to be exchanged, the HHS regulations makes no sense.

This tautology extends beyond the courtroom to the real world. ONC's current approach creates an insurmountable engineering barrier to meaningful progress. It is why ONC-sponsored health data exchange projects are and will continue to be unsustainable, and have and will fail over the course of 2013.[12]

The absence of data exchange standards has an impact beyond HITECH implementation. It is also, for example, the fundamental obstacle to efforts of the Department of Defense and the Veterans Administration to enable their respective health record systems to exchange medical record data for the benefit of service members and veterans.[13] The continuing costs of this interoperability barrier in outcomes and dollars are well known. They are the target of oft-renewed efforts by the secretaries of both departments. Yet DOD-VA efforts, like a raft of health information exchange projects in the civilian sector, are unlikely to succeed until ONC

---

[11] For an example from the field of securities regulation of the intersection of an agency's substantive statute with the Administrative Procedure Act, 5 U.S.C. § 551 *et seq.*, resulting in the invalidation of agency action, see *Business Roundtable v. SEC*, 647 F.3d 1144 (D.C. Cir. 2011). (SEC's 2010 proxy access rule vacated because of deficiencies in the SEC's rulemaking process, due to inadequate cost-benefit analysis).

[12] *Cf.* Hon. Lamar Alexander, et al., *Letter to Hon. Kathleen Sebelius*, Apr. 16, 2013, available at www.thune.senate.gov/public/index.cfm/files/serve?File_id=04df (requesting, *inter alia*, information on progress under $250,000,000 in cooperative agreements with "Beacon Communities"). The site for the Beacon Community Cooperative Agreement program is http://www.healthit.gov/policy-researchers-implementers/beacon-community-program .

[13] *See generally, Statement of Valerie C. Melvin, Director, Information Management and Technology Resource Issues,* United States Government Accountability Office, Testimony Before the Committee on Veterans Affairs, U.S. House of Representatives, GAO-13-413T (February 27, 2013) (analysis of the failure of the Department of Defense and the Department of Veterans Affairs to develop an interoperable health record system despite being required to do so by Act of Congress).

takes a different approach to the architecture of health information exchange. We need an architecture we can actually build, and so turn next to that task.

## 4. Planning Successful Health Information Exchange Through a Simplified, Achievable Network Architecture

We refer to ONC's technological approach as a *provider-query-based network architecture*. The theory of this architecture is well known. A patient presents (appears) at a doctor's office or hospital (the point of care). The doctor sends a computer query to all EHR (Electronic Health Record) data bases locally, regionally, or nationally. The query asks all the data bases whether they contain information about the patient in question. All EHRs that can identify the patient and that hold such information are asked to send it securely to the point of care. There it is assembled immediately so the treating physician can use it for treatment.

Alternatively, a *provider-query-based network architecture* can in theory be built using an additional, intermediate component – a master index database. In this theoretical structure, every provider locally, regionally, or nationally must send every entry in every EHR for every patient to an index kept by a computer. Each entry specifies that the provider's medical record database contains an entry for each given patient. Every time a provider sees a patient and makes an entry, a message reflecting that entry is sent automatically to the local, regional, or national index.

The index is itself a huge database that grows constantly and rapidly. It is always available to doctors, hospitals, and other providers. When a patient presents at a point of care, the doctor, hospital, or other provider sends a query message to the index database. The index database sends queries to every physician's or hospital's database which has listed an entry for the patient in question in its EHR. The EHRs each send all the data for that patient to the index, which then transmits all those entries to the point of care. The computer system at the point of care then assembles all the messages it receives through the index into a comprehensive record for the patient. The treating physician or hospital in theory then has a current, compiled medical record in its own EHR to use to treat the patient.

The provider-query-based blueprint is elegant in outline. The problem is that we lack the technology to make it work.

This lack has been demonstrated repeatedly. It is the lesson of the well-known Santa Barbara demonstration project[14], for example, though many who analyzed that debacle failed to understand how the selection of a provider-query-based network architecture made success unattainable. Among other things, the architecture created substantial privacy, security, and safety problems that proved insoluble. It was also a lesson taught repeatedly in projects sponsored by ONC during the eight years of George W. Bush's administration (though ONC did not recognize that lesson in its projects). It is a lesson that will be taught again this summer as ONC-sponsored Health Information Exchange (HIE) projects, including the "Beacon" projects, continue to fail across the country. We believe that almost none of those projects will prove

[14] *See* Robert H. Miller and Bradley S. Miller, *The Santa Barbara County Care Data Exchange: What Happened?*, *Health Affairs* 26, no.5 (2007):w568-w580, available online at http://content.healthaffairs.org/content/26/5/w568.full.html .

workable, sustainable, or scalable. This is a harsh reality and bespeaks a huge waste of federal and matching money.

ONC and the nation need an alternate system architecture that uses existing technology to facilitate the interchange of health information among the hundreds of thousands of existing EHR computer systems installed in doctors' offices and hospitals around the country. The exchange system must specify a data format protocol to enable the vast existing EHR base to send patient data back and forth in a form usable by physicians, nurses, and others. The data format protocol must be technically feasible in the short term, such as within a year.

There is a temptation at this point to wish that any system ONC specifies must be able to exchange data with a high level of semantic interoperability. (Semantic interoperability is the ability of two or more computer systems to exchange information and have the meaning of that information accurately and automatically interpreted for use by the receiving systems.)[15] In a future health IT network with very highly developed semantic interoperability, computers could exchange health data reliably and interpret the data as well. That would require, in colloquial terms, compatibility among the computers' transmitting and receiving methods (protocols) and a pervasive use of common ontologies (structured vocabularies) covering all or most of the health data exchanged, plus the capability to exchange free (unstructured) text. This is an ideal vision of health data exchange that may be developed years in the future.

Technology available in the short term is not that capable, however. Useful and more realistic – but still robust – data exchange goals are therefore a practical necessity. That must become a guiding principle if Congress expects ONC to start down the path toward a workable health exchange architecture. That shift to the pragmatic is essential to getting widespread health data information networks up and running in the near future, however that time frame is defined. In this important sense, technological limitations control the policy options that Congress can mandate with a realistic expectation that the mandates will actually be carried out.[16]

*In systems design, the key to connecting patients' health record bank accounts and providers' various EHR systems is, from the outset, to restrain the societal urge to try to do too much – to require what available technology cannot support. The federal government's systems design choice must respect the limits of interconnection technology. It must seek the achievable. So far ONC and its Policy Committee have not done that.* Reboot *catalogs the dismal consequences.*

Thus, until ONC is convinced or otherwise forced to change its choice of network architecture based on the criterion of technical feasibility, its policies will continue wasting time, effort, and money. Moreover, its programs' failures will continue impairing the ability of

---

[15] Explanations of semantic interoperability and its prerequisite, syntactic interoperability, are available from many sources. *See, e.g.,* EN 1306 Association, *Semantic interoperability of health information*, available at http://www.en13606.org/the-ceniso-en13606-standard/semantic-interoperability .

[16] *See Statement of Valerie C. Melvin, supra* n.13, at 7: "[T]he National Defense Authorization Act (NDAA) for Fiscal Year 2008 included provisions directing VA and DOD to jointly develop and implement, by September 30, 2009, fully interoperable electronic health record systems or capabilities." In 2013, no such system exists and the two departments remain stymied in their efforts to fulfill this mandate. *Id.* at 17.

patients, providers, insurers, and others to exchange health information in digital form efficiently and affordably.

Fortunately, a technically achievable architecture exists for nationwide exchange of digital health information. The most efficient way to organize digital health records for nationwide exchange is to integrate them around the patients to whom they pertain. Each patient's records can be stored in secure repositories ("health record banks") in accounts where access is controlled by the patients themselves. This solves myriad privacy and security issues that are insurmountable using provider-query architecture.

Doctors, hospitals, and other providers would still maintain their own office or institutional records to document their internal clinical processes and the care they give to each patient. Vendors of current Electronic Health Record (EHR) systems would continue selling and improving their products. Providers and hospitals would be able to continue using the vast base of clinical record systems already bought and installed. That is true even though, today, those systems cannot routinely exchange digital records because they are operationally incompatible and thus not "interoperable."

As we explain below, the more practical, achievable systems design respects the proven limits of interconnection technology. That means making policy decisions to design a system that initially will achieve a very modest, rather than a high, level of interoperability. However, even the modest level of interoperability we suggest will be a signal improvement over the status quo, a quantum jump; and it will get the interoperability process out of the present quagmire.

The architecture we suggest therefore uses a variant of "Direct"[17] an interconnection methodology suggested to ONC as a stopgap and then developed with ONC's encouragement and assistance. Direct is capable of using a health record exchange format, the Continuity of Care Document (CCD). CCD is based on Extensible Markup Language (XML), which is well known and widely used. The CCD already has robust data exchange capabilities; it embodies significant progress towards creating semantically interoperable, essential clinical data.[18]

---

[17] Information about the Direct Project is available at http://www.healthit.gov/policy-researchers-implementers/direct-project .

[18] *See, e.g.*, National Institute of Standards and Technology (NIST), *Meaningful Use Test Method*, available at http://healthcare.nist.gov/use_testing/finalized_requirements.html, and listing, *inter alia*, under Certification Criteria at §170.306(f), *Exchange clinical information and patient summary record* (pdf), Aug. 13, 2010). That document, *Test Procedure for §170.306.f Exchange Clinical Information and Summary Record* (Approved Version 1.0, August 13, 2010), specifies:

> Standard. Health Level Seven Clinical Document Architecture (CDA) Release 2, Continuity of Care Document (CCD) (incorporated by reference in §170.299). Implementation specifications. The Healthcare Information Technology Standards Panel (HITSP) Summary Documents Using HL7 CCD Component HITSP/C32 (incorporated by reference in §170.299).

*Id.* at 4. Thus, HITSP C32 is the version of the CCD in use. Version C32 offers substantial semantic interoperability by virtue of extensive accommodation of standard vocabularies, specified in detail in the test procedure that follows, *id.* at 10-18. *See also*, HITSP, *C 32 –*

Because CCD is an exchange format that works today, its selection for current systems design purposes is the essence of practicality.

In the systems design we propose, health record banks and EHRs in doctors' office and hospitals would be required by federal rule to have the capacity to write to and read from a central communications backbone that would be available nationwide. This is called a "publish-subscribe" backbone (or hub). Messages written to or downloaded from the backbone would be addressable (akin to electronic mail).

The common standard for exchanging data over the Direct or Direct-like backbone would be the XML-based Continuity of Care Document (CCD). This is an industry standard format.[19] CCD is constantly being improved yet is of great utility in its current iteration.

Using the CCD would enable significant interchange of appropriately formatted medical record data and other health information in digital form. It would not enable digital encoding of all information that physicians and hospitals will record in their institutional EHRs, but it would enable a level of interoperability that is both far beyond the status quo and of significant help to patients and providers who participate in the exchange.[20]

One objection to this patient-account-health-data-repository architecture is that physicians and other providers will distrust any health records that they do not control, and especially will distrust health records compiled in patient-controlled repository accounts. This

---

*HITSP Summary Documents Using HL7 Continuity of Care Document (CCD)*, available at http://www.hitsp.org/ConstructSet_Details.aspx?&PrefixAlpha=4&PrefixNumeric=32:

> The Summary Documents Using HL7 Continuity of Care Document (CCD) Component describes the document content summarizing a consumer's medical status for the purpose of information exchange. The content may include administrative (e.g., registration, demographics, insurance, etc.) and clinical (problem list, medication list, allergies, test results, etc) information. This Component defines content in order to promote interoperability between participating systems such as Personal Health Record Systems (PHRs), Electronic Health Record Systems (EHRs), Practice Management Applications and others.

[19] Background about the Continuity of Care Document is available at, e.g., http://www.hl7.org/implement/standards/product_brief.cfm?product_id=6 and http://www.hitsp.org/ConstructSet_Details.aspx?&PrefixAlpha=4&PrefixNumeric=32 , among many sources.

[20] Patient Command has long been in favor of this approach to health network exchange architecture, even before Direct was first suggested to ONC. *See* B. Strom, R. Marks, W. Knaus, *Letter to Hon. Kathleen Sebelius*, (May 6, 2009). The later proposes that HHS and ONC implement HITECH using a national health data architecture based on integrating data around patients. The patient-focused integration would be accomplished via patient-controlled health record bank accounts. The letter proposes interconnecting the patient-owned and controlled accounts to institutional EHRs through an XML backbone and using the CCD. The letter is available on the website of the Health Record Banking Alliance at http://www.healthbanking.org/docs/PComm%20ARRA%20RuleM%20Ltr%20SecHHS%20050609.pdf . The letter illustrates that the fundamental task under HITECH – first developing and publishing federal interoperability standards – has not changed since the day HITECH was signed into law.

objection is overcome because health record banks can label each data input to a patient's record with the provenance (source of and transmission path for) the particular data entry. That way, physicians and others can make a clinical evaluation of each data element they consider in evaluating and treating a patient. Moreover, the health record bank's software can help identify conflicts or other anomalies in the compiled data.[21]

Providers will readily become accustomed to using data they receive, or are authorized to import, from patient-controlled health record bank accounts. Further, physicians and providers will always be able to conduct their own up-to-date evaluations, repeat tests if that appears warranted, and rely on their own institutional records about a given patient. The societal advantages of having patient-controlled medical data compilations is so compelling that we believe providers will quickly adjust to using them, with appropriate cautions. Enabling patients to be part of their own care team will bring myriad benefits.

We believe that a pivot to this architecture can reboot the federal government's health IT initiative. It can make HITECH work. A patient-account-health-data-repository architecture using a publish-subscribe backbone and the Continuity of Care Document as the principal content protocol sounds complicated. It is, however, attainable using available technology.

This pivot would suddenly make development of sustainable health record banks achievable. Consumers, acting directly or through their health record banks, would have an automated way to extract medical record data from their providers' EHRs and move it easily, without any transcription, into their health record bank accounts. They could also with ease send extracts from the data compiled in their health record bank accounts to various providers, family members, and other advisors. The data would be stored and exchanged securely. The architecture would ameliorate many of the daunting security problems ONC has failed to overcome, because patients would be able to exercise dynamic access control, i.e., they would make privacy decisions access-by-access as circumstances dictated.[22]

---

[21] *See* W. Knaus, *Health Records for Safer Care – Faith, Hope, and Reality (How Consumers Now Can Control their Medical Information and Help Physicians Provide Better Care)*at 5-6, 14-15 (Sidebar - Characteristics of a Personal Health Record that Will Make It Useful to Clinicians as an Accepted Supplement to Their Institutional Medical Record) (White Paper, Feb. 25, 2008), available on the Health Record Banking Alliance site at http://www.healthbanking.org/docs/White%20Paper%20Faith%20022508.pdf. For additional analysis about overcoming physicians' reluctance to use compiled medical records stored in health record banks, *see* R. Marks, *Regulating Personal Health Records – Why HIPAA Won't Work*, at 4-5 (eHI Policy Paper, 2008) (discussing in detail issues of clinical credibility and utility for compiled medical records in Personal Health Records (PHRs)),available on the Health Record Banking Alliance site at http://www.healthbanking.org/docs/eHI%20Policy%20Paper%20v1pdf%20090108.pdf.

[22] Background about health record banks (including a short introductory video) is available at the site of the Health Recording Banking Alliance, http://www.healthbanking.org/ . A December 12, 2012 white paper on health record bank business models, *Health Record Banking: A Foundation for Myriad Health Information Sharing Models*, and a January 4, 2012 white paper, *A Proposed National Infrastructure for HIE Using Personally Controlled Records*, are available at the site. (For disclosure purposes, Richard D. Marks is Vice President of the Health Record Banking Alliance.)

Vendors of existing EHR systems would need to add the publish-subscribe (write-read) capability mandated by the federal standard. Then their EHR systems' records could be output into the Continuity of Care Document format (including XML-based free text for narratives in patient's digital records). They could also receive CCD input through the backbone for input into their systems' EHRs.[23]

---

[23] The recent announcement from a group of prominent industry vendors of The CommonWell Health Alliance illustrates how the lack of a HITECH-mandated data system interoperability standard continues to slow vendors' progress in developing capacities to communicate among various brands of institutional EHRs. CommonWell is a consortium of some, but not all, major vendors of institutional EHR systems. Its website is http://www.commonwellalliance.org/ . CommonWell's announced purpose is to promote development of health industry data exchange standards – the very requirement mandated for ONC in Section 3000(13) of HITECH. CommonWell is thus a telling industry response to ONC's failure to adhere to the statutory requirement to develop a data exchange interoperability standard. We note again for emphasis that such a standard is the prescribed statutory foundation necessary to achieve all subsequent HITECH goals.

In any case, CommonWell announced that membership in its consortium was open to other health IT industry vendors. CommonWell became controversial, however, almost as soon as it was announced. Epic, one of the largest and most successful health IT system vendors, charged that it was excluded from the consortium. As one article reported:

> Epic Chief Operating Officer Carl Dvorak had more harsh words for CommonWell, calling it a 'marketing opportunity,' according to *Forbes*. Dvorak added that he doesn't think Epic would join the alliance, and *said the company, instead, would prefer for a national standard to be set.*

D. Bowman, Epic *CEO: CommonWell being used as a 'competitive weapon,'* FierceEMR, March 7, 2013 (emphasis supplied), available at http://www.fierceemr.com/story/epic-ceo-commonwell-being-used-competitive-weapon/2013-03-07. Thus CommonWell's formation raises competition questions that remain open and may presage the possibility of litigation.

In addition, and more significant for near-term progress, CommonWell's likelihood of success in developing comprehensive data exchange standards acceptable to the entire health industry is open to substantial question. This is apparent from reported comments of CEOs of two CommonWell consortium members:

> Healthcare's going through significant change, all of us know it. We're living through it,' McKesson CEO John Hammergren said. 'We believe that one of the key challenges we face is not just automated healthcare, but connecting it together. Over time, we've done a good job as an industry automating our silos, but we've not done a very good job of collaborating across the silos and developing the connectivity … the data liquidity necessary to make that happen.
>
> '*This interoperability mission is really an imperative for us. We know that it's going to take significant work.*'

Engineering these system capabilities will be straightforward for some system vendors, expensive and time-consuming for others, and attainable by all. It is a practical first step because Direct as far enough along in its development. We will address in the next section how use of Direct can be simplified by modifying the current approach to authentication issues under Direct.

## 5. Adopting Authentication Measures in Health IT Compatible with Incremental Societal Developments

In *Reboot*, the authors note:

> No system is completely invulnerable to criminals or reckless actors who do not follow protocols. As systems become more secure, they may be less useful to providers and patients. Therefore, concerns about the security of patient information need to be balanced against the burdens placed on entities that are responsible for the safekeeping and disclosure of the data. It is unclear if HHS has properly considered the safety and security issues, much less the burden, to date.[24]

These considerations come into play regarding the identity management and authentication system for Direct. This is a technically complicated security subject. The question is whether ONC should allow Direct to adopt a special set of authentication standards for Direct called DirectTrust[25], or mandate instead that Direct use authentication technology that is likely to be gradually adopted more widely.

---

> Cerner CEO Neal Patterson *called the collaboration a beginning, saying that the government has not and is not going to deal with the problem of interoperability.*

D. Bowman, *Cerner, McKesson and other EMR rivals form interoperability partnership,* FierceEMR, March 5, 2013 (emphasis supplied), available at http://www.fierceemr.com/story/cerner-mckesson-and-other-emr-rivals-form-interoperability-partnership/2013-03-05.

The CommonWell Consortium is but the latest of many industry initiatives. They all respond in one way or another to the same deficiency. It is a recognition that engineering a nationwide health IT data exchange *requires* ONC to develop the interoperability standards demanded in HITECH, and an acknowledgement that ONC remains mired in its own misconceived processes and is unlikely to develop those standards any time soon.

CommonWell – in its early stages, unproven, and saddled from the start with charges of anti-competitive conduct – is no substitute for ONC's changing course and fulfilling its duty to develop interoperability standards as the essential initial step in HITECH implementation.

[24] *Reboot* at 22.

[25] The site for DirectTrust, "an independent non-profit trade association created by and for participants in the Direct community," is http://www.directtrust.org/.

One such authentication option is the identity management trust framework set up under a federal government committee infrastructure.[26] So-called approved trust framework solutions exist under this approach consistent with OMB and NIST guidelines.

The General Services Administration manages the Identity, Credential and Access Management (ICAM) program that uses credentials (e.g., tokens such as smart cards) that enable various levels of security authentication (or levels of assurance).[27] These tokens are already available for purchase outside the federal government. In time ICAM could become a widespread, relatively inexpensive means for individuals inside and outside government to establish identity credentials for a governmental, commercial, and social uses. Another option for health care is to adopt the identity standards developed by the NIST-sponsored Identity Ecosystem Consortium based on the National Strategy for Trusted Identities in Cyberspace (NSTIC).[28]

---

[26] The Identity, Credential and Access Management (ICAM) Subcommittee was established in 2008 by the Federal CIO Council's Information Security and Identity Management Committee (ISIMC) is http://www.idmanagement.gov/pages.cfm/page/ICAM .

[27] From the GSA website at http://www.gsa.gov/portal/category/26757 :

> Identity, Credential and Access Management (ICAM) is the intersection of digital identities and associated attributes, credentials and access controls into one comprehensive approach.
>
> The OCIO ICAM Division is responsible for coordinating ICAM activities across GSA by:
>
> - Supporting GSA Access Card issuance, usage and lifecycle maintenance for GSA personnel
> - Developing GSA-wide identity, credential and access management solutions
>
> The ICAM Division was originally established to help GSA comply with the Homeland Security Presidential Directive - 12 (HSPD-12). This directive requires that all federal agencies adopt common, reliable and interoperable identification standards for employees and contractors. The ICAM Division safeguards GSA assets by ensuring that all GSA personnel obtain Personal Identity Verification (PIV) credentials, and by developing enterprisewide, compliant, identity solutions. GSA branded the PIV credential it issues to its employees and contractors as the 'GSA Access Card.'

[28] The NSTIC website is http://www.nist.gov/nstic/. NIST Special Publication 800-63-1, *Electronic Authentication Guideline*, available at www.nist.gov/itl/csd/sp80063-121311.cfm, states in the Executive Summary at vi:

> These technical guidelines supplement OMB guidance, *E-Authentication Guidance for Federal Agencies* [OMB M-04-04] . . . . OMB M-04-04 defines four levels of assurance, Levels 1 to 4, in terms of the consequences of authentication errors and misuse of credentials. Level 1 is the lowest assurance level, and Level 4 is the highest. The OMB guidance defines the required level of authentication assurance in terms of the likely consequences of an authentication error. As the consequences of an authentication error become more serious, the required level of assurance increases. The OMB guidance provides agencies with the criteria

For purposes here, we suggest only that oversight activities resulting from *Reboot* consider whether directing ONC to mandate a standard, widely used authentication methodology for Direct is a better approach than the customized methodology being pursued by DirectTrust.

In all events, Congressional oversight should recognize that identity management and authentication are security problems confronting society at large. Adopting a network architecture for health information exchange can benefit from identity management systems developed for government or industry generally, but creating unique or specialized authentication frameworks under HITECH is unnecessary. For ONC to develop or even support specialized healthcare authentication strategies would add unnecessary complication to an already formidable task.

## 6. Conclusion – Navigating the Bipartisan Politics of Successful Nationwide Health Information Exchange

As Congress performs oversight and considers the virtues of ONC's pivoting to successful new health IT exchange architecture, we suggest keeping in mind these factors to help assess interoperability standards:

- Patient engagement through control of access to their compiled health information from all their providers.
- Dynamic (ongoing) patient privacy control to give consumers confidence in their control of access to their compiled health data, an important privacy concern.
- Technical feasibility in the short term, as reflected in a simplified network architecture that uses technology available today.
- Connecting disparate legacy EHR systems using a "publish and subscribe backbone" ( a hub or bus) using the current iteration of the XML-based Continuity of Care Document (CCD) as the initial vocabulary exchange standard which is proven, available, and amenable to evolution.
- Affordability and cost-effectiveness, both system-wide and for small providers.
- Ability to facilitate patients' access control over their own health data for participation in research under informed consent and the Common Rule by making available both identified and de-identified information as patients may elect through dynamic access control.

Health IT is complex enough. Adding unnecessary complexity by continuing to chase the wrong network architecture will only further frustrate ONC's progress and the industry's.

Congressional oversight can succeed by basing health IT policy on unambiguous experience under the George W. Bush and Obama administrations: nationwide health information will not succeed until and unless HHS adopts a network architecture that integrates data around each patient. The inherent efficiencies of that design are in undeniable contrast to the insurmountable inefficiencies, privacy and security concerns, and unaffordable costs of a "provider-query" network design.

---

for determining the level of e-authentication assurance required for specific applications and transactions, based on the risks and their likelihood of occurrence of each application or transaction.

Successful oversight will succeed only if Republicans and Democrats join in these conclusions. The incentive is there for political collaboration on health IT policy, because delay and unnecessary cost in ONC's performance span the stewardship of both parties.

Bipartisan cooperation on interoperability standards offers the potential for structural change in the market for healthcare. Easy, affordable health data exchange can alter the market behavior of patients and the providers who must respond to them.

When consumers have access to the information in their own medical records, they will make smarter choices in purchasing health care and managing their health. That means systemic health care costs are very likely to go down while outcomes improve. That great prize is at stake in the *Reboot* oversight initiative.

Respectfully submitted,
PATIENT COMMAND, INC.

By: *Richard D. Marks*

Richard D. Marks
President

Contact Information:
richardmarks@earthlink.net

**Comments of Patient Command, Inc.**

## Appendix
## Schematic Comparison of Health Information Infrastructure Architectures

## Provider-Query Architecture *versus* Patient-Centered Repository (Health Record Bank) Architecture

### Provider-Query Architecture

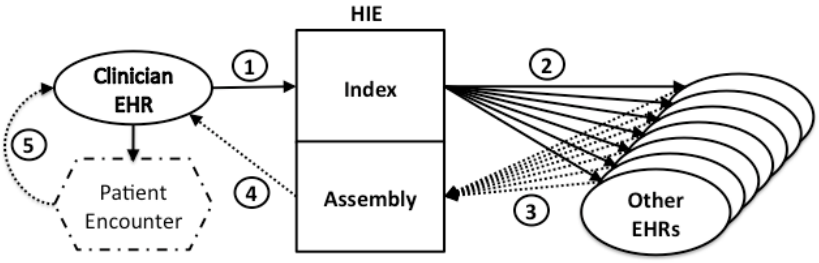


**Figure 1. Institution-centric Community HII Architecture.**

1. The clinician EHR requests prior patient records from the HIE; this clinician's EHR is added to the index for future queries for this patient (if not already present)
2. Queries are sent to EHRs at all sites of prior care recorded in the HIE Index; patient consent is verified at each "other" EHR prior to release of information
3. EHRs at each prior site of care return records for that patient to the HIE; the HIE must wait for all responses
4. The returned records are assembled and sent to the clinician EHR; any inconsistencies or incompatibilities between records must be resolved in real time
5. After the care episode, the new information is stored in the clinician EHR only

### Patient-Centered Repository (Health Record Bank) Architecture

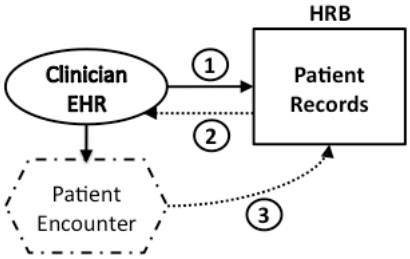


**Figure 2. Patient-centric Community HII Architecture.**

1. The clinician EHR requests prior patient records from the HRB
2. The prior patient records are immediately sent to the clinician EHR
3. After the care episode, the new information is stored in the clinician EHR and sent to the HRB; any inconsistencies or incompatibilities with prior records in the HRB need to be resolved before that patient's records are requested again (but not in real time)

(Note: This process is repeated whenever care is provided, resulting in the accumulation of each patient's records from all sources in the HRB)