Electronic Health Record Interchange

A Response to the Federal Government's Request For Information on the Development and Adoption of a National Health Information Network

Brian Deasy
Senior Consultant
CapTech Ventures, Inc
804-545-8743
bdeasy@captechventures.com

Mr. Deasy has seven years' experience as a computer systems consultant, including four years consulting for large health insurers. He holds a B.S. in computer science from the College of William and Mary.

CapTech Ventures, Inc. is a technology company that uses software engineering processes to solve complex business problems for a wide range of clients including Fortune 500 companies, Federal and State government agencies, and regional market leaders.

Contact Information

Charles A. (Sandy) Williamson
CEO and Co-Founder

Slaughter Fitz-Hugh
COO and Co-Founder

CapTech Ventures, Inc
1419 West Main Street
Richmond, VA 23220
Phone 804.355.0511
Fax 804.355.4220
www.captechventures.com

CapTech Ventures, Inc
(Technology Lab)
1118 West Main Street.
Richmond, VA 23220
Fax 804.355.2591

Business Contacts

Sandy Williamson
Phone 804.545.8701

Brian Deasy
Phone 804.545.8743

GSA Contract Number

GS-35F-0330P

1. Introduction

By now, many interested parties within the health care industry, federal, state, and local governments, and the public at large are aware of the recent attention paid by the federal government to the promise of interoperable electronic health records (EHR). The capacity to store a patient's complete medical history in electronic format, and to exchange all or part of it electronically between health care providers in real-time, is arguably the most effective way to deploy information technology to meet the twin goals of improved patient care and cost control in the health care sector.

The present focus on EHR began on April 27, 2004 with President Bush's creation of the Office of the National Coordinator for Healthcare Information Technology (ONCHIT). The primary directive assigned to the new office was clear and ambitious: to provide all Americans access to an electronic medical record within 10 years. Within 90 days ONCHIT released a federal "Health IT Strategic Framework," calling for a coordinated national effort to "inform clinical practice, interconnect clinicians, personalize care, and improve population health." And now, in early 2005, ONCHIT has opened the door for public comment on how best to shape that national effort by issuing a Request for Information (RFI) regarding the development and adoption of a national health information network.

In the time these events have unfolded, work has already begun on the myriad elements required to establish such a network. Indeed, many of these efforts were already quietly in progress before the spotlight turned their way. Standards groups such as HL7, SNOMED, and others have advanced their work already in progress to define vocabularies and communication formats for interchange of EHR data. Vigorous discussions regarding sticking points such as the relative need for a unique patient identifier have sprung up in policy and industry circles. And, perhaps most importantly, increasing numbers of individual communities have begun incubating their own regional EHR interchange systems (now commonly referred to as Regional Health Information Organizations, or RHIOs.) As of January 2005, eHealthInitiative, a public-private partnership working for the advancement of interoperable health information technology, listed 133 health information exchange efforts in its community database.[1]

In this same time period, "conventional wisdom" regarding the challenges associated with EHRs has also begun to take root. As with all conventional wisdom, some elements – the inability of small provider practices to meet an unfunded mandate for implementation of EHRs, for example – are well justified. As also frequently happens, however, some aspects of the conventional wisdom regarding a national EHR initiative are overly pessimistic. Some forces that have the potential to help drive adoption have been underappreciated, while some technical barriers have been overblown. In addition to addressing many of the questions posed in ONCHIT's RFI, this paper will highlight these overlooked opportunities. Ultimately, we feel a realistic

[1] Foundation for eHealthInitiative, "Connecting Communities for Better Health: Community Directory," http://ccbh.ehealthinitiative.org/communities/states_search.aspx (accessed January 18, 2005).

assessment of the tasks, risks, and opportunities the health care industry faces on the road to broad adoption of EHRs gives cause for cautious optimism.

2. Requirements of a NHIN

Before proceeding further, our own working definition of a National Health Information Network (NHIN) must be established. As with all well-specified systems, it helps to start by defining the requirements. An effective NHIN must:

1. Offer providers (physicians and facilities) real-time, on-demand access to a patient's medical history at the point of care, regardless of where the events included in that history (physician orders, lab results, surgical procedures, prescriptions filled) physically took place.
2. Provide patients access to their own medical record.
3. Facilitate administrative simplification and cost control in a variety of healthcare processes:
    - Reduction of redundant tests and services
    - Increased efficiency in the transmission of medical data not just between providers but also to and from payers and consumers
    - Decreased redundancy in the storage of patient data among and within organizations
4. Enable the extraction of de-identified, aggregate data suitable for the needs of government agencies involved in the Federal Health Architecture (FHA). For example, real-time epidemiological data should be available to the CDC's National Electronic Disease Surveillance System (NEDSS), while flexible extraction of in-depth data on arbitrary services, procedures, or conditions should be available for further analysis by the Agency for Healthcare Research and Quality (AHRQ). Properly planned for, this aggregate data could also enable the EHR interchange network to operate as a medical "expert system," providing physicians real-time feedback as to the most effective test or tests for confirming a given diagnosis, serving to further reduce costs related to unnecessary testing. Such a system might even help guide physicians to the proper diagnosis when unusual combinations of symptoms are observed.
5. Restrict access to this data in accordance with HIPAA regulations. In particular, the NHIN must guarantee that persons or entities viewing personally identifiable data have the patient's express authorization, with reasonable exceptions in the case of emergency intervention when the patient cannot provide authorization.

3. Technical Features of a NHIN

Later we will examine specific technical features that might underpin a NHIN. At this time, armed with the requirements enumerated above, we can paint a broad functional picture to inform the rest of our discussion.

- **A NHIN will be defined regionally, not nationally.** Certainly, in the end, regional efforts should be linked nationally, and to ensure linkage is feasible it must be planned for now. But the majority of the benefits of EHR implementation accrue immediately from implementation at the regional level. Because most people move

from one geographic region to another infrequently, and most patient care occurs within the patient's own community, sharing information locally will meet most requirements right off the bat. A purely regional health information exchange can offer providers and patients secure access to large portions of a patient's medical record. Properly planned for, stand-alone regional implementations can even provide extraction of de-identified, aggregate data for public policy purposes, although admittedly the lack of an integrated NHIN would hamper efforts of inherently real-time activities that are national in scope, such as counter-bio-terrorism surveillance.

That one caveat notwithstanding, we will go so far as to say that even framing the effort in terms of a **national** health information network is really putting the cart before the horse. What is needed is a national effort to foster regional health information exchanges. In practice, it appears ONCHIT is already well aware of this concern and is approaching the task as such, but the point cannot be overstated: any effort to force immediate standardization nationally for interchange format or, especially, technical architecture is doomed to collapse under its own weight as regions struggle more with meeting national guidelines than building networks that effectively meet their regional needs. On the other hand, an approach that allows vigorous regional experimentation offers a good chance of success. For our own part, we will use the terms NHIN, RHIO, and the more general "EHR interchange" somewhat interchangeably in this paper, with the understanding that a NHIN will really exist primarily as an interconnection of RHIOs.

- **Within a NHIN, heterogeneous regional implementations will expose a standard external interface to the national network.** It will be crucial to allow varying implementations at the regional level for years to come, as this will be the best means to arrive at robust, scalable architectures that will be suitable for widespread adoption. National connection of regional implementations should not wait for widespread adoption and standardization before commencing, however. The solution to this conundrum is for the national backbone to standardize on a single architecture and format, while anticipating the need for translation to and from its standards as data is passed between participating RHIOs. This approach will clearly come at a cost. Even the best data mappings between competing medical records standards will not be perfect, so some information may be lost in translation. Some member RHIOs may not be able to translate patient identifiers effectively enough that they can answer every national request. However, accepting these shortcomings now for the sake of allowing varied regional approaches will ultimately result in a better NHIN two, five, and ten years from now. For the next several years, when the goals of regional variance and national interconnection find themselves at odds, regional variance should be given precedence.

- **A NHIN will be based upon open standards.** The barriers to participation in a RHIO and therefore a NHIN must be as low as possible, in both a business sense and a community sense. Vendors need to be able to create innovative products that compete in the marketplace based on sound architecture, robustness, and reliability – not based on proprietary vendor lock-in. Health care organizations will have enough to worry

about when facing governance and coordination issues -- they need to be able to choose from a variety of vendors and feel free to implement their own regional variations, secure in the knowledge that standards for interoperability between their selected platforms and the wider world are clearly specified. When we say that regional implementations may vary, we still anticipate and suggest the communication formats and interfaces between systems in those regions be based on open standards.

- **A NHIN will include Physicians, Facilities, Pharmacies, Payers, and Consumers**. It has been generally (and logically) assumed that physicians and facilities will be at the core of EHR interchange. Pharmacies are also frequently included within the assumed scope of EHR efforts, since the capacity for e-prescribing to reduce potentially catastrophic medical errors is well recognized. Consumers have a clear right to access their own data, and such access will further the cause of disease management and consumer-directed health care plans. Payers are often marginalized or left out of plans altogether, however. We feel strongly that this is a mistake. Given the opportunity, payers will play an important role in EHR efforts for a simple reason: they have financial incentives to do so. We will elaborate on these financial incentives in the "Drivers" section below.

- **The data exchanged on a NHIN will continue to reside on source systems.** Data should remain on the source systems (practice management systems, hospital computerized patient record systems, etc) and be made available for rendering to other participants, rather than being duplicated in a central repository or on other participants' systems. This serves multiple purposes:
    - Reduces implementation costs by avoiding redundant storage mechanisms
    - Reduces complexity of implementation by avoiding duplicate information within the network
    - Reduces governance concerns by avoiding ownership and liability issues surrounding a central repository

- **NHIN data will be available on demand to participants in the network.** The flip-side of foregoing a central repository is the need for real-time availability data from source systems. Many of the benefits of a RHIO will be compromised if the data takes more than, say, 90 seconds (at worst) to retrieve. Therefore data must be immediately available to authorized individuals on a real-time basis. Governance bodies should establish mutually agreeable service level agreements (SLAs) up front to ensure maximum availability of data.

4. Drivers

The requirements and technical features listed above are ambitious. They will require close cooperation and significant financial investment from healthcare entities and multiple levels of government. It is valid to ask whether the financial and social benefits outweigh the costs, and if the requisite level of cooperation and commitment is really achievable. The answers to these concerns can be addressed only after reviewing the stakes of those involved.

4.1. Payers

As we have already mentioned, we feel payers are a largely overlooked force for adoption of EHR interchange. The conventional wisdom runs like this: "Physicians and facilities bear the cost implementing EHR, but do not reap the financial benefits." The conclusion from this is not to throw up our hands, but to identify who will reap the financial benefits, then solicit and encourage financial support from those entities. Payers have direct financial incentives to encourage EHR. These incentives take two forms:

- **Payers have the most vested interest in reducing costs related to redundant medical care**. A variety of forces are afoot to move health care to a more consumer-driven model, thereby creating more traditional economic incentives for controlling costs. One recent estimate placed the number of Americans enrolled in consumer directed health care (CDH) plans at about 2.6 million as of January 1, 2005, more than double the number enrolled in such plans at the same time the previous year.[2] Even with such an impressive adoption rate, however, 2.6 million is a tiny fraction of the overall American population, and it is clear the traditional payer-provider relationship will remain prevalent in the healthcare marketplace for some time to come. This being the case, payers are a largely overlooked source of funding for EHR interchange initiatives.

  Patients and providers both have weak or, in some cases, counter-incentives to enforce cost savings. Patients face inconvenience from duplicate testing and, indirectly, lower wages or higher health care premiums out of pocket. They do not generally face a significant financial deterrent to waste at the time of care, however. Providers can benefit from the workflow improvements offered by EHR adoption (less time spent collecting patient history and so forth) and pay a penalty for duplicate testing in the form of increased workloads in an already strained and chaotic environment. In a well-ordered suburban setting, however, a case can be made that from a strictly financial perspective doctors actually benefit from those same increased workloads and the redundant payments that result.

  Ultimately, in a traditional, non-CDH health care transaction it is payers that have the strongest incentive to avoid waste, as well as the accounting and data-analysis resources to recognize the costs they suffer due to waste. In a landmark move, in July 2004 BCBS of Massachusetts announced a $50 million investment in a pilot program to connect one Massachusetts community with interoperable EHRs, and closely study the resulting benefits and costs. One of the primary reasons cited by BCBSMA was the asymmetrical cost/benefit calculation between payers and providers regarding adoption of EHR interchange.[3] Other forward-looking payers already actively spend money partnering with providers to reduce overhead costs by encouraging web-based and HIPAA EDI interaction, preempting telephone calls to expensive call centers.

---

[2] AIS Consumer-Directed Care, "CDH Growth and Enrollment Projections," Atlantic Information Services, Inc., http://www.aishealth.com/ConsumerDirected/CDdata/CDGrowth.html (accessed on January 18, 2005)
[3] Marianne Kolbasuk McGee, "$50 Million Plan To Give One Community E-Health Records," *Information Week,* (July 8, 2004) http://www.informationweek.com/story/showArticle.jhtml?articleID=22104465 (accessed January 18, 2005)

These payers face an even stronger business case for eliminating direct costs due to redundant care, and should be willing to put cash on the line to support that goal.

- **EHR interchange would also allow payers to reduce internal administrative costs, further lowering the cost of healthcare to the insured**. Payers currently expend a great deal of effort duplicating and transferring what amounts to medical record data between claims, medical management, disease management, and wellness screening systems. These systems cannot and should not be replaced overnight. However, as systems reach the end of their natural life cycles, it will make sense for payers to build and adopt new systems based on the same EHR models and standards emerging in hospitals and physician practices. This step, combined with payers' involvement in EHR interchange networks with the capacity to take a "raw feed" of a patient's EHR, will allow payers to perform multiple operational functions from a single, integrated data store. HIPAA transactions and codesets have begun fostering an environment hospitable to direct EDI between providers and payers. Building on that to ultimately exchange patient data in medical record format presents a path to greater fulfillment of the HIPAA promise of administrative simplification.

4.2. Physicians

While the virtues and deficiencies of the American medical system can be debated, one of the most admirable aspects of the system is the commitment of its physicians to supplying quality care to those in need. While financial imperatives can often interfere (doctors must ultimately be paid for their services in order for the system to function) or even conflict (as noted above, strictly speaking, more demand for medical care is of financial benefit to physicians) we believe the vast majority of American doctors favor the adoption of tools that result in better patient care. Thus, the potential for EHR to reduce errors by providing a complete and timely medical record at the point of care is of great interest to physicians.

Moreover, EHR interchange does not need to rely solely on doctors' altruism for their support. EHRs and EHR interchange are classic cases of information technology freeing professionals to spend more time doing what they originally entered the profession to do – in this case, helping patients. By automating the propagation of a patient's medical information from one care setting to the next, a doctor can spend less time collecting and transcribing patient histories that, often as not, are still fragmented, incomplete, or redundant despite all the manual effort that goes into them. In exchange, these physicians can spend more time analyzing the accurate clinical data from past incidents, discussing points of concern in more depth with the patient as needed, and ultimately arriving at better informed courses of treatment. Clearly, this helps the doctor and the patient.

We feel this qualitative improvement in the practice of medicine has been underestimated as a driver for EHR adoption. Organizations adopt technology because it helps the bottom line, whereas individuals tend to purchase technology because they appreciate the impact it has on their everyday lives. Physician practices, while they are financial organizations that must attend to the bottom line, are fundamentally personality-driven and responsive to individual needs. Given sufficient support in the form of low-interest loans or, in cases

of more demonstrable hardship, grants, physicians will opt for the chance to improve their daily working lives and patient care at the same time.

4.3. Facilities

Health care facilities, like individual physicians, have a strong dedication to providing quality care. Being corporate entities, however, they also often have a greater awareness of and attentiveness to the bottom line. This works in favor of EHR adoption, as the larger, institutional nature of facilities fits well with the capacity for EHRs to promote cost savings. In contrast with smaller physician offices that may realize qualitative gains from health care information technology (HIT) adoption but have difficulty justifying the initial investment, many facilities have already realized financial benefits from computerized physician order entry (CPOE) and computerized patient record (CPR) technology. Indeed, many (but certainly not all) facilities have already implemented some forms of EHR interchange, most often amongst hospitals operated by the same company in the same community. Regardless of whether a facility is currently exchanging medical records with another organization, regional EHR interchange with their affiliated providers offers an efficient way to extract additional value out of CPOE and CPR systems.

4.4. Pharmacies

Pharmacies offer value to their customers by fast, efficient fulfillment of their prescriptions. Through e-prescribing supported by a RHIO, prescriptions can be filled ahead of time quickly and efficiently at the patient's pharmacy of choice without their involvement. Though the same benefits can accrue to the patient through phone transactions, an electronic data interchange (EDI) solution offers productivity and workflow gains to both clinicians and pharmacists. Perhaps more importantly, the involvement of pharmacies in a RHIO serves two other important goals:

- e-prescribing aids the public interest by dramatically reducing the chance of medical errors due to illegible hand-written prescriptions
- Including prescriptions and subsequent refill data in a patient medical record helps complete a physician's understanding of patient care. A doctor can better address a patient's treatment if she is aware that patient has not picked up his medications. This same information can also shape effective disease management.

4.5. Consumers

Putting consumers in a position of power to impact the cost and effectiveness of health care is one of the primary goals in the health care industry today. Giving patients access to their medical data can serve the patients' interest and impact the industry in a number of positive ways:

- **Assist the consumer in understanding complex incidents of care.** Interested patients should have the power to understand and participate in their own care. The first step is a single view of what has actually been done to and for them.
- **Give the patient a longitudinal view of their own health.** Putting a patient's medical record in front of them is a good first step towards engaging them in making themselves healthier and therefore reducing future health care costs**.** Even better would be for the medical record to offer links to informational resources or even self-

directed disease management features that enable the patient to easily take further steps towards improving their health.

- **Access to provider performance data to improve outcomes and reduce costs.** This item is controversial because it has the potential to scuttle cooperation between all the parties necessary to make a RHIO succeed. However, if a goal of a RHIO is truly to improve the health system as a whole through cost reduction and improved patient care, it cannot be ignored. In the aggregate, the data accessible through a RHIO can facilitate competition amongst providers and assist in the standardization of care by indicating which providers obtain positive outcomes at reasonable costs. The different parties to a RHIO will have very different feelings regarding what data should be available and how it should be presented, but RHIO governance bodies need to have the hard conversations up front to reach mutually agreeable goals and policies on publication of this sort of data.

4.6. Governments

The concept of portable electronic health records is not new. One of the reasons that previous efforts to foster widespread adoption in the industry have not taken root is because "for the public good" has a hard time showing up on a balance sheet.
While we feel strongly that the bottom-line interests of several parties have been underestimated historically, it has become clear that the final push required to reach a critical momentum towards EHR adoption must come under government auspices. Governments have a number of reasons to take steps in this area:

- The oft-cited figure of 48,000-98,000 deaths per year in the United States due to medical errors[4] is oft-cited for a reason. It is too high – at its upper end, more than twice the number of fatalities due to car accidents (about 42,000[5]) and nearly five times the death toll from intentional homicide (about 20,000).[6] Governments put a great deal of effort into reducing the murder rate and ensuring that our highways are as safe as possible; it is reasonable to expend a small fraction of that same effort on reforming the safety of the medical system.
- Governments, as custodians of public health, have an interest in extracting de-identified, aggregate health information on a regional and national scale for a number of reasons: scientific research regarding public health, monitoring against epidemics of infectious disease, and recognizing and reacting to a biological or chemical terrorist attack.
- In its role as the representative of the people, government has a responsibility to encourage reform in a medical system that is un-responsive to market controls. The uninsured have no one working on their behalf to reduce costs. Insured individuals have payers negotiating fee schedules with providers, but economic incentives are too roundabout to provide effective cost regulation. In general, payers charge employers who may or may not choose to pass on costs to employees in the form of increased

[4] Agency for Healthcare Research and Quality, "Translating Research Into Practice: Reducing Errors in Health Care," http://www.ahrq.gov/research/errors.htm (accessed January 18, 2005)
[5] National Center for Statistics and Analysis, http://www-fars.nhtsa.dot.gov/
[6] Centers for Disease Control, "Deaths and percentage of total deaths for the 10 leading causes of death, by race: United States, 2001," http://www.cdc.gov/nchs/data/dvs/nvsr52_09p9.pdf (accessed January 18, 2005)

contributions to annual premiums, reduced benefits, or even reduced wages. Employees have no way to know what their health insurance is truly costing them. In a system where even the wealthiest individuals could scarcely afford treatment for many illnesses if they were paying directly, the capacity for individuals to impact the cost of care has been lost. RHIOs and the exchange of EHRs will create an immediate reduction of costs through reduction of redundant care, availability of information to aid consumer-directed healthcare and disease management, and positioning of the industry for further cost-savings through effective use of an integrated view of patient data. Encouraging adoption of EHRs is an effective way for government to help reform the system without over-involvement or heavy handed regulation.

With this broad survey of the various stakeholders' interests in mind, we can restate our case for cautious optimism. Payers are a largely untapped resource for leadership and financing. Physicians have an overlooked desire for qualitative gains that can be facilitated through modest government incentives. Facilities can leverage and expand existing CPOE and CPR systems that have already proven their value to incorporate EHR interchange. Consumers stand to gain a greater understanding of and voice in their own treatment, and governments have an alignment of goals and responsibilities that is driving them to put the right incentives in place.

5. Overcoming Technical Barriers

Even with the convergence of interests enumerated above, serious technical barriers to workable EHR interchange remain. It is impossible to state for certain at this point in time what approaches will work best for overcoming each of these hurdles. This is exactly the reason we stress that regional experimentation must be allowed and encouraged over the next several years, to allow the relative strengths and weaknesses of technical solutions to emerge over time. But we would not suggest organizations adopt EHR interchange if we didn't feel that workable solutions currently exist for the major technical concerns. While some implementations may turn out to be more effective than others, no implementations are doomed to failure. Below is a discussion of some of the major technical issues we foresee, and a survey of possible solutions.

5.1. Performance

The response time of an EHR interchange network, particularly a NHIN operating on a national scale, is a major concern. To satisfactorily meet functional requirements, the network must be able to return a complete patient history while a physician waits at a bedside. Thus far, various RHIO implementations have experimented primarily with peer-to-peer and hub-and-spoke architectures.

- In a **peer-to-peer** architecture, requests are propagated amongst member systems directly, without the use of any centralized server. This technology, most often associated with controversial music-sharing systems, is actually quite powerful and should not be dismissed because of its shady roots. The primary advantage of a peer-to-peer architecture is reduced cost; little or no additional hardware beyond existing client systems is required.

- A **hub-and-spoke** architecture incorporates a central server into the mix. Actual patient data may not be stored on the hub, but all requests are directed from client systems to the hub and then re-distributed to all or some of the other client systems. The amount of processing performed on the hub could vary widely: it could simply pass all requests onto all clients (its value over a peer-to-peer system is then debatable) or it can perform a variety of tasks to manage the traffic on the network.

Peer-to-peer networks are a fascinating and promising technology, deserving of further development and experimentation. It is our feeling at this time, however, that hub-and-spoke architectures offer a variety of advantages over peer-to-peer. They have the capacity to boost performance, and they position the architecture to take advantage of other technical features, such as public key infrastructures, that will be enumerated later. The responsibilities of the central hub could include:

- **Central point for authentication, authorization and data protection activities.** Usernames, passwords, and second-factor authentication criteria can be stored securely. Meta-information about participants (such as medical practice and facility names, etc) would be readily available. While avoiding the replication of detailed patient data, the hub can store high-level patient demographic data as well as securing patient encryption keys. The hub could also perform filtering of requests so that a patient need not grant access to all of their medical history to all physicians that treat them. A dentist might be restricted to other dental information and the family physician might be restricted from viewing psychiatric records. More detail on these security activities is provided in the security section below.

- **Aggregation of "directory" data.** The hub could store references to which client systems contain information on which patients. This can dramatically improve performance, as requests from one provider could be routed only to systems that actually contain data for the patient. Long running requests to particular clients could be terminated if need be, and status information on the request can be supplied back to the original requestor along with response data. For example, a response might include a number of incidents of care, along with a statement that Dr. Smith was unable to respond in a timely fashion and Children's Hospital was not available at all. Such additional data, difficult or impossible to provide in a peer-to-peer architecture, can provide valuable sanity checks to use of the system. Users will have enhanced capacity to understand why they are not getting the results expected if certain records do not show up.

  This directory data concept applies at the regional and national level. In fact, the propagation and application of this data is conceptually similar to the underpinnings of the TCP/IP networking protocol. National hubs could store "gateway" style information, indicating that they may not know the final systems to query but they do know that some system downstream of their nearest neighbor has information on patients A, B, and C, while preventing pointless requests for patient D's data from propagating onto that network segment.

- **Support for local caching.** Hub data stores might optionally associate "most recently updated" flags with directory data. This would allow clients to locally cache previously requested data and only replace it with new data when it is available. This mechanism would operate similarly to the caching mechanisms available in the HTTP protocol. The capacity to locally cache data would insulate network clients from "I know it was here last time I looked" syndrome. If a single provider in the network experiences an outage of their system, clients that had recently retrieved their data could still have it on hand.

5.2. Security

Security issues can be divided into a number of distinct concerns:

- **Authentication** involves proving *who the user is* – is the user stating she is Mary Smith of Dr Jones' practice truly who she says she is? This is one of the less challenging aspects of EHR interchange, as a number of robust, straightforward authentication strategies are available. The most simple, of course, is the familiar username/password combination. For a sensitive system such as an EHR network, however, so-called two-factor authentication should be applied. In a two-factor authentication scheme, the user must offer two pieces of data to prove their identity – typically something the user knows combined with something they have, such as a physical card or token. Most often the first factor is a simple password, paired with any number of second factors (listed in order of increasing cost):
    - a digital certificate stored on a PC or handheld device
    - RFID-tagged or bar-coded company ID badge
    - RSA SecurID or other token
    - smart card
    - biometric supplied via a fingerprint, hand, eye, or facial scanner.

  Because of the need to keep barriers to entry low, a simple digital certificate is probably the best choice, although there is no reason authentication mechanisms cannot vary regionally or even location by location, as long as basic security protocols are followed.

- **Authorization** is the related but distinct concern of *what a user may access*. Once we are confident that a user is in fact Mary Smith, whose medical records should she be able to view? This is one of the largest hurdles to successful implementation of a NHIN or RHIO. The fundamental problem is the conflict between two basic requirements:
    - **Patients must have control over granting access to their own data**. Medical information is private and must remain so in any RHIO or NHIN. Medical personnel treating a patient should have access to that patient's history if permission is granted by the patient, but a curious neighbor should not be able to bring up someone's medical records simply because they work in the health care industry.
    - **The system must not rely upon patients to carry any password or physical authentication mechanism to access their data.** Experience in the European Union has shown that portable medical records systems

based upon patients physically transporting their histories with them on smart cards are failing because, among other reasons, patients cannot be relied upon to bring the histories with them to every medical encounter.[7] Certainly patients cannot be expected to have the medical cards on them at all times in case of emergency – in the case of a traumatic accident, even if the patient originally had the information with them it may have been lost or destroyed. Functionally, it makes no difference if the physical data was in the patient's care or only if the patient was entrusted with a smart card containing a digital certificate or even a simple password – users may not carry the smart card or may forget a password, and in any event an unconscious victim cannot provide a password.

So, given the inherent tension between these two concerns, how can a workable system be devised?

The best approach is to employ a public key infrastructure (PKI). In a PKI system, two keys exist for each entity (in this case, each patient), a public key and a private key. Data encrypted using the public key can only be decrypted using the private key, and vice versa. Such a system can be used, for example, to send and receive trusted email. A sender can encrypt or "digitally sign" their outgoing message with their private key. A receiver can decrypt the message using the sender's public key, which is widely known and available. In this direction, anyone with the public key (which is not intended to be kept a secret, so one should assume anyone might have it) can read the message, so it is not secure in that sense. However, because only the sender's public key can unlock the message, whoever reads it can be 100% certain the sender was the person whose public key they used to read it.

The same keys can be applied in reverse – if a sender encrypts a message with the intended recipient's public key, only that receiver will be able to unlock that message, by applying their private key. In this direction, the sender can be certain their message will be read only by its intended recipient.

Such PKI systems are mature and robust – typically the most complex issues surrounding implementation involve not the technology itself but the management of the public and private keys to achieve the desired behavior within the system. In fact, the "infrastructure" in "Public Key Infrastructure" refers to the necessary framework surrounding issuance of keys from a Certificate Authority (CA), allowing for revocation of keys if a private key is compromised, etc. Again, models for this infrastructure are well established. Of course, in our case we don't want to send emails. But by mixing a combination of advanced technical security and administrative audit trails the same technology can be employed to meet the requirements of secure access to patient data in an EHR interchange network, through application of the following process:

[7] Todd Stein, "U.S. shouldn't bet on smart cards," Healthcare IT News (Daily News - October 18, 2004). http://www.healthcareitnews.com/NewsArticleView.aspx?ContentTypeID=2&ContentID=1746 (accessed January 18, 2005)

1. A patient presents himself to a provider affiliated with a RHIO. The patient signs the appropriate HIPAA-compliant forms granting the provider access to his medical records. Optionally, the system could support granting only partial access to the medical history based on groupings of provider specialties specified by the patient during this step. Any restrictions specified would be enforced by the hub during later searches.
2. At this point administrative personnel in the provider's office log on to the EHR interchange network, satisfying all authentication requirements.
3. The administrative personnel uploads a digital copy of the HIPAA form to the hub of the EHR interchange network along with patient identifying information. The hub performs a patient matching procedure and determines if this is a new patient (has never seen a participating provider) or a returning patient (has previously seen another provider in the interchange network.) If the patient is new, the system generates a new public/private key pair for the patient. If the patient is already in the system, a key pair will be on file. The private key associated with the patient is added to that provider's access list. The digital copy of the HIPAA authorization form is stored with event data associating that user of the network with the authorization to view that patient's medical records.
4. Users associated with that provider's office may now initiate searches for that patient's data. A search message, including the patient's public key as an identifier, can be sent to the hub. The hub verifies the provider office is associated with that patient's private key and therefore authorized to perform searches. If so, the hub encrypts the request using the private key and forwards it on to providers holding information on that patient. The request now consists of an envelope with the patient's public key, and contents encrypted using the private key. Note that at no point did the private key actually have to leave the secure confines of the hub.
5. Any network participant receiving a search request can decrypt it using the public key attached to the request. If the decryption works, they can be certain the request is valid, that is, it came from a participant who had been granted access to the patient's private key. They can then respond to the request with the patient's data, optionally encrypting it with the patient's public key for additional security on the trip back to the central hub.
6. As the response is routed back through the hub, the hub can safely decrypt the response for the "last mile" trip back to the requesting provider. Communication pipes between the hub and providers will be secure in and of themselves (see "Data Integrity" section below.) By decrypting the responses on the hub, the security of the private key is maintained by eliminating the need to distribute it to an individual provider for decryption on site.

The key feature of this approach is that the provider only has access to the data because they were associated with the user's private key, and that association with the private key has a clear audit trail provided without the use of any additional

technology, knowledge, or presentation of physical object required by the patient.

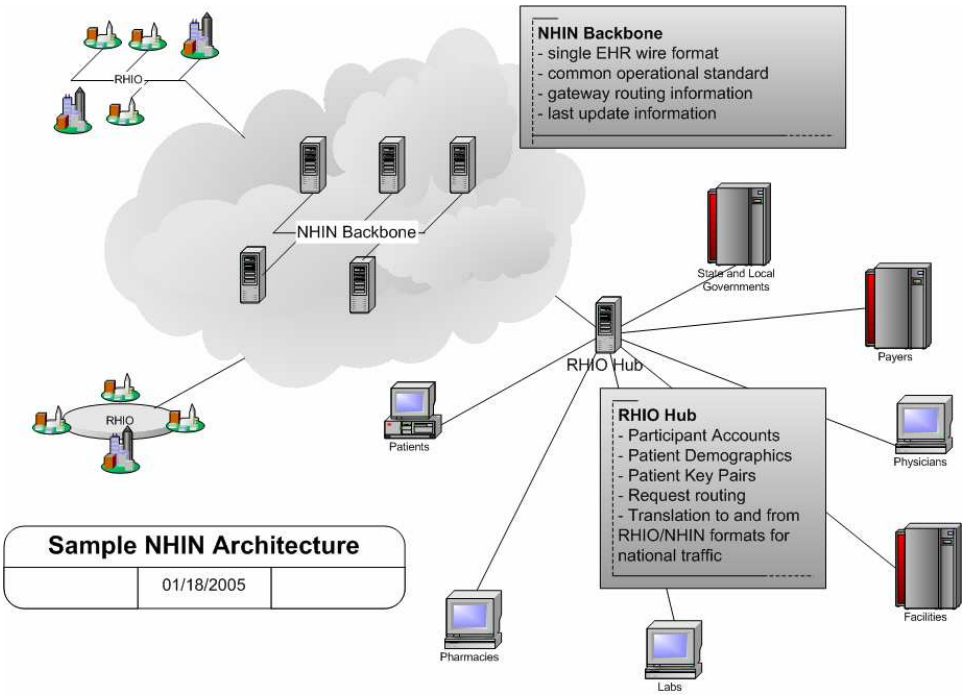
A further benefit of this strategy is the capacity for network participants to contribute to a patient's medical record without gaining access to that patient's history. For example, a lab facility can store the patient's test results and respond to requests from other providers using the patient's public key, without ever requiring access to the patient's private key.

Is this procedure open to human failure or sophisticated "social engineering" fraud? Yes, but no more so than the existing paper-based system – it is in fact better, with a clearer audit trail to deter potential fraud.

- **Data Integrity** addresses the security of data during storage and transmission. How can we prevent malicious persons from gaining access to the data outside our expected authentication scheme, either while it is in-place in a provider's office or during transmission? This is a strength of modern IT systems and as such, not a major challenge to EHR interchange implementation. All communication within the EHR interchange network should be performed using secure sockets layer (SSL) encryption. Over and above the PKI encryption scheme detailed above, SSL connections create secure data "pipes" that help prevent man-in-the-middle attacks from intercepting data during transmission and, more importantly, prevent such attackers from reading the transmitted data even if it is intercepted. As far as in-place security on each of the host systems attached to the network, this is non-trivial but is also a major focus of mainstream vendor software and, at any rate, exists as a concern independent of EHR interchange.

5.3. Patient Matching

A major concern for EHR interchange is how to tie together patient data created at different times in different settings. As patient data accrues over time, how can a distributed system ensure that each new piece of data is associated with the correct person and, equally important, does not wind up associated with the **wrong** person. A white paper published by CapGemini in September of 2004 citing the lack of a unique patient



identifier as the single greatest hurdle to EHR implementation[8] fueled a continuing debate within the health care community over the need for a unique identifier and the political feasibility of creating one. Our position is a simple one:

- A unique identifier would greatly simplify implementation of EHR interchange. Social security numbers, supplemented by an ID issuance system to cover small segments of the population, such as illegal immigrants, that may not have a SSN or equivalent government-issued number, would be an ideal choice for such an identifier.
- Due to political concerns beyond the control of a mere technical consulting firm, use of the SSN or any new, government issued unique healthcare identifier is not a realistic option anytime in the near future.

So, no use crying over spilt milk. How, then, to implement effective patient matching logic without the service of a unique patient identifier? Through the application of the PKI mechanisms suggested in our Security section above, we are actually already halfway there. Patient key pairs should be stored in the hub system along with certain identifying information. At a minimum, this information should include:

- patient first and last name
- date of birth
- gender
- address (current address should be associated when a patient is first configured; prior addresses should be retained over time as patients move)
- ID number for health insurance plan (again, current and prior data should be stored for maximum effectiveness)

Leveraging the PKI system, patient match must be performed only when a patient is associated with a new provider. The patient can provide their identifying information and that information can be matched against data stored on the interchange network hub. At this time, if need be multiple ambiguous matches can be returned to the provider for clarification with the patient. The most effective patient match algorithms are open for further study and debate, but the most important feature is that a perfect match is not a requirement. *Once a patient match is performed and the patient's key pair is identified, the public key can be associated with that patient's data in the provider's system*. Future searches circulate the patient's public key on the network; the public key becomes a de facto patient identifier within the scope of this interchange network, and any other network that shares the same key-issuing certificate authority. This system has a number of advantages:

- Fallible patient matching on demographic data is performed infrequently, always with the option of human intervention.
- Data entered into the system is clearly associated with a unique individual, substantially reducing the risk of "mix and match" patient histories with multiple people's histories intermingled. Of course, such situations can and will still occur occasionally, and a mechanism must be built into the system to arbitrate these concerns, but we feel the infrastructure specified here will increase the reliability of data to a workable level.

[8] Peter Kongstvedt, M.D., John Quinn, and Hindy Shaman, *Health Information Technology and the Electronic Health Record: Implications for Healthcare Organizations* (CapGemini Consulting, 2004)

- The convenience of a unique identifier is approximated without many of the privacy and security concerns:
    - Public keys are too unwieldy (256 characters long, when using hexadecimal notation for a 1024 bit key, the current industry standard) to be used for other purposes. They run little or no risk of "scope creep," unlike social security numbers.
    - The public keys need never be stored, printed, referred to, or otherwise used outside the software of the EHR interchange system. Even if the number were to be posted publicly, no harm is done and nothing is compromised. A third party gaining access to a person's public key cannot access that person's medical history (the private key, as well as authenticated access to the EHR network, would be required to even attempt to gain unauthorized access to a patient's history.) An additional benefit of keeping the keys "inside the system" is the capacity to easily revoke and reissue a patient's keys if the original private key is compromised, or change all patients' keys at will if the network changes its certificate authority (as it might choose to do to increase interoperability with other networks.)

5.4. Interoperability Standards

Data interchange cannot occur without standards – clearly both participants in a transaction must speak the same language. Beyond this basic requirement, there are a number of touch-points within a potential NHIN to which standards must be defined and enforced if an integrated network is to succeed. Starting from the bottom up, these touch points are:

- **Medical records in provider source systems (practice management systems and computerized patient record systems).** Standardization of data within the source systems is not a requirement, but is desirable. In particular, open medical records standards that are "EHR interchange ready" and open source implementations of record systems that utilize those standards will significantly aid adoption amongst poorer physician practices in rural and urban areas. The open source OpenVistA[9] and VistA-Office[10] implementations of VistA, the Veteran's Administration's electronic medical record system, are appropriate moves in this direction.

- **Wire-format for an Electronic Health Record.** This is the format an incident of care will be represented in as it is transmitted from one network participant to another. Of course, this format is absolutely crucial. HL7 has already issued a draft standard of one candidate.[11] It is not absolutely required that only one standard exist at this early stage, however. As long as standard mappings between competing transmission formats can be defined, different regions can agree upon different formats within their

[9] More information on the Open VistA initiative by the Pacific Telehealth and Technology Hui can be found on the Internet at: http://www.pacifichui.org/projects/disp_proj.cfm?proj_id=76

[10] More information on the VistAOffice EHR software joint venture by CMS and VHA can be found on the Internet at: http://www.cms.hhs.gov/quality/VistAQsAs.pdf

[11] More information on the HL7 EHR System Functional Model Draft Standard for Trial Use (DSTU) can be found on the Internet at: http://www.hl7.org/ehr/

region, and assume responsibility for translating their local format to the NHIN standard at their connection point to the NHIN. These mappings will certainly not be ideal. But the advantages of allowing implementations to proceed now, without long wait times on the "perfect" standard, plus the opportunity for regional experimentation with different formats to help inform that future "perfect" standard, outweigh the drawbacks of accommodating multiple formats on the network. Allowing and anticipating the use of multiple standards circulating on the network will also position the NHIN to accommodate rapid upgrade cycles to new versions of a particular standard. That is, improvements to a given standard such as the HL7 EHR System Functional Model can be approved and published quickly, and standardized mappings between the newer and older version can be released simultaneously. With these mappings included as part of the new standard, individual regions can take advantage of the new versions quickly without fear of losing interoperability with the rest of the network.

- **Operational standards.** The discussions and recommendations outlined in this document represent one point of view. Successful systems can and will be built using other architectures. Similar to allowing multiple wire-formats, a successful NHIN will not mandate a one-size-fits-all operational model. As long as requests can be meaningfully propagated onto a regional network segment and a response can be communicated back to the NHIN backbone, the specific conventions of that regional segment should be immaterial. That is, the backbone must define a single expected wire format, security scheme, and request mechanism. But regional organizations should be free to input that format at a single touch point onto their network, alter it to operate on their network, collect the pertinent responses, and reply to the backbone in the expected format.

  For example, a NHIN could adopt the hub-and-spoke, PKI-based architecture outlined in this document, but an attached region might operate a peer-to-peer, decentralized system with its own patient matching algorithms. That region could input national requests, map the public-key based ID to whatever equivalent they have implemented, initiate a peer-to-peer request locally, and submit the results of that local request back to the NHIN backbone. As long as the region can "speak" the correct formats to the backbone and respond in the prescribed amount of time, how the request was satisfied should be immaterial to the NHIN infrastructure.

  As with translations between multiple wire formats, allowing operational variability will have drawbacks: some RHIOs may not be able to effectively map patient ID schemes, while others might not support the required response times. Again, the benefits of regional variability outweigh these concerns.

6. Conclusion

There are many challenges ahead on the road to widespread adoption of EHR interchange. In this paper we reviewed many of those challenges and outlined the approaches we feel will best overcome them. Some of our approaches have not received a great deal of prior attention, such as greater involvement of payers as a source of funding

and the application of a public key infrastructure for patient identification and authorization of medical record access. Others are well-traveled ground, such as the need to start at the regional level, and to employ open standards as the building blocks for an integrated National Health Information Network. More important than any single approach to any given challenge, however, is the need to seize the moment that has been offered to the healthcare community to act in the interests of all its stakeholders and move forward with EHR interchange adoption. We applaud the efforts of the Office of the National Coordinator for Health Information Technology towards this end, and trust that is exactly what the industry will do.

Appendix A: Cross-reference to RFI Questions

1) **Working definition of a NHIN** is addressed in sections 2 and 3.
2) **Broad-brush operational model for a NHIN** is addressed in section 3.
3) **National vs. Regional responsibilities** are addressed in sections 3, 5.1, and 5.4.
4) **Stakeholders and governance framework** are addressed in section 4.
5) Not addressed
6) Not addressed
7) **Privacy and security concerns** are addressed in section 5.2.
8) **Accomplishing public policy objectives** is addressed in sections 2, 3, 4.6, and 5.4.
9) **Encouraging private sector competition** is addressed in 3, 4.5, and 5.4.
10) **How to encourage the NHIN to be privately funded, non-proprietary, interoperable and innovative** is addressed in sections 3 and 5.
11) **How to encourage utilization and broad adoption regardless of means** is addressed in sections 3, 4, and 5.
12) **How regional efforts will be impacted** is addressed sections 3 and 5.4.
13) Not addressed
14) Not addressed
15) Not addressed
16) Not addressed
17) **The management approaches and rules required to promote interoperability standards** are addressed in sections 3 and 5.4.
18) **The appropriate roles for the federal government** are addressed in sections 3, 4.6, and 5.4.

