CONNECTING FOR HEALTH℠

MARKLE FOUNDATION *A Public-Private Collaborative*

ACHIEVING ELECTRONIC CONNECTIVITY IN HEALTHCARE

Summary of Recommendations

Technical Panel

July 2004

MARKLE FOUNDATION

THE ROBERT WOOD JOHNSON FOUNDATION

Technical Panel Summary of Recommendations

In order to provide a majority of their benefits, clinical applications must interconnect with other clinical systems. The potential to avoid medical errors and drug interactions, to deliver real-time prompts and reminders at the point of care and directly to the patient or caregiver, and to improve the ability to conduct clinical research depend on a highly connected network of regional healthcare communities that exchange data between effectively used clinical systems such as EHRs.

Unless there is purposeful attention paid to infrastructure requirements at the local, regional and national level, it is unlikely that piecemeal technology adoption will result in the connected infrastructure necessary to realize the quality of care and economic efficiency gains promised by IT. The network requires a high degree of connectivity that arises from trust, safeguards for privacy and security and a strategy that minimizes risks of patient data misuse. With that said the approach must be voluntary and built on the premise of patient control and authorization.

In order to accelerate electronic connectivity, a non-proprietary "network of networks" that is based on standards and a decentralized and federated architecture should be developed, building upon local and regional networks. To support the creation of the network where national standards are implemented locally and regionally, a "Common Framework" is needed immediately.

The "Common Framework" is comprised of standards, policies and methodologies that can be replicated quickly related to secure connectivity, reliable authentication, and a minimum suite of standards that work together to support information exchange. We recommend that the common framework be tested and evaluated through a reference implementation to be completed in the short-term to enable rapid progress.

Because our incremental approach is designed to leverage existing infrastructure it dictates that secure connectivity be built on the Internet and its communication protocols. Part of the function of the "Common Framework" is to select security standards for confidentiality, authentication, integrity and non-repudiation (CAIN). The "Common Framework" also addresses reliable authorization, a common set of standards and a minimum set of capabilities required to participate in the network.

To enable rapid implementation of the network of networks, emerging financial and other incentives should incorporate aspects that promote the usage of the standards-based interoperable health information infrastructure as well as clinical applications, such as electronic health records, electronic prescribing tools, and other clinical applications that utilize standards. Care should be taken to only promote those applications that do not represent "dead-ends". Certification of both applications and interfaces that emerge as part of the common framework will be needed to align incentives with standards-based IT.

Among the important implications of our proposed system for a network of networks, is that personal health information would continue to reside where it does now, primarily with hospitals and healthcare providers. According to the patient's preferences, relevant health data could be assembled from numerous sources at the point of care, enabling decision making to be informed by past treatment successes and failures and medication history. Both the patient and the clinician could have direct access to this vital information.

A new infrastructure element would be an index of pointers to where patient information is located, but which contain no personal health information; no patient records would be stored

centrally. Decisions about sharing information would be made at the "edges" of the network by patients and providers together on a case by case basis.

The secure and confidential treatment of patient information is a fundamental design criterion of the health information infrastructure we endorse. We recommend the inclusion of architectural, technical, and policy safeguards within the "Common Framework", to safeguard the privacy and security of patient data while at the same time permitting the rapid and accurate exchange of information among authorized users. Proposed steps for safeguarding privacy and security are embedded in the fabric of all of the *Preliminary Roadmap* recommendation areas.

An important principle of our technical work is the need to leverage the potential of information technology through incremental efforts. We cannot simply shut down the healthcare system and rebuild it from scratch. Such an approach would be dangerously disruptive and prohibitively expensive. All of the technical recommendations of Connecting for Health assume an incremental migration toward the end goal of a truly interoperable healthcare system.

Finally, as noted above, we propose the development of one or more public-private pilot projects or "reference implementations" within the next 12 months in order to test and refine our technical recommendations, further specify the "Common Framework" and promote the rapid adoption in a responsible manner.

Detailed Technical Panel Recommendations

1. Infrastructure

a. **Develop the health information infrastructure in a way that safeguards privacy, leverages both bottom up and top down strategies, is incremental in nature and based on a decentralized and federated model--** an interoperable, standards-based "network of networks" **built on the Internet.** The network should not contain a central repository for patient medical records. Instead, it should be a pathway that facilitates their identification and exchange in a private and secure way with appropriate authorization. (See the draft illustration of the proposed infrastructure at the end of this document.)

b. **A "Common Framework" is needed immediately in order to pursue a decentralized strategy that builds out from a local and regionally driven approach to creating the infrastructure.** Only by conforming to a Common Framework can we ensure that data exchange pilots, personal health records, and regional systems will be able to interoperate across and with other regional systems. The "Common Framework" is premised on secure transport over the Internet and provides minimal but basic components for the infrastructure including secure connectivity, reliable authentication, and a minimum suite of standards for information exchange. It is comprised of network software, common policies, documents and methodologies that can be shared in the public domain.

c. **Public-private collaboration should fund and complete a Reference Implementation within 12 months. The Reference Implementation is a complete implementation of the "Common Framework."** Until a fully functional example of the "Common Framework" exists, ambiguities and gaps will remain in the definition. The Reference Implementation should execute a complete implementation of the common framework in a "live" regional or state pilot project. This reference implementation will serve several purposes, including:
   - Prove the feasibility the "Common Framework"
   - Enable the testing and evaluation of standards, policies, and specifications with the goal of replicability
   - Develop and disseminate a low-cost implementation model.
   - Provide a test-bed for certification of systems to be connected to the exchange.

Guiding Principles (Infrastructure):

1. **Safeguard Privacy:** In order to be accepted by patients and providers, the network must safeguard the privacy of health information. Trust is a crucial component of the doctor-patient relationship, including those elements of the relationship that involve the disclosure and sharing of sensitive information. If sensitive information is disclosed inappropriately then trust in both the provider to whom the information was entrusted and the network will be lost. Participation in the network must be voluntary and must be built on the premise of patient control and authorization.

2. **"Bottom Up" and "Top Down":** The debate surrounding the formation of a health information infrastructure does not necessitate a stark choice between local and national initiatives. The strategy for implementing the *Roadmap* includes both top-down and bottom-up elements. Most healthcare is local, and the bulk of information transfer occurs in a patient's own community. Many multi-institution systems, that are effectively local health information infrastructures, already exist. However, a common framework must be in place to ensure interoperability between those systems as they grow. The common framework will also permit each individual's personal health record to interact with the network of electronic health records in any and all communities.

   As with the growth of the fax network or the Internet, the bulk of the IT implementation will be undertaken locally, in response to local needs and resources. By basing the network on standards, the system will work with a variety of hardware and software thus saving participating institutions from being forced to adopt a 'one size fits all' solution. Given the "Common Framework," the market will create solutions that are appropriate for small physician practices, multi-hospital institutions, families and other participants. These standards also assure support for stakeholders such as public health that by their nature extend beyond any one locale.

   Ultimately, it is desirable to leave to the local systems those things best handled locally, while specifying at a national level those things required as universal in order to allow for interoperability among regional systems. In particular, the minimum security standards required to assure secure Internet transmission or patient matching methods must be national, so that all participating institutions can connect to one another securely and without unworkable variation.

3. **Avoid "Rip and Replace":** The requirements of economic sustainability and practicality demand an evolutionary approach and a clear migration path for all participants in the health information architecture. Given the non-stop demands of providing healthcare services, change must evolve incrementally.

   Any proposed migration path must take into account the current structure of the healthcare system, and must work with that infrastructure where possible. Some of this infrastructure will need to be replaced, of course, and the replacement and migration will generate new costs, if only during the transition period. Where possible, however, the system should include what has been deployed today.

4. **Decentralization**: Data stay where they are. The U.S. healthcare system is fragmented. Many types of institutions exist as part of the current healthcare network, from giant hospital systems to individual practices, with all manner of specialists, clinics, and agencies in between. We do not believe there will be any wholesale change by

2010. Therefore, any proposed improvement to the healthcare system must assume that the participants will be decentralized and must accommodate voluntary, partial, and incremental participation.

The decentralized approach leaves clinical data in the control of those providers with a direct relationship with the patient. This approach greatly reduces the risk of misuse by ensuring that there is no single "bucket" holding identifiable clinical data, and leaves judgments about who should and should not see patient data in the hands of the patient and the physicians and institutions that are directly responsible for the patient's care.

The decentralized approach also reflects the legal and market realities of healthcare. If institutions were required to share all of their data to participate (as is the case with some existing centralized approaches), many would choose not to do so.

Of course, the network facilitates the transfer of selected information from one end point of the system to another, as is required for providing care and supporting informed patient participation in care. The decentralized approach obviates the need for storing identifiable data in a central database. Even though the infrastructure is decentralized it still supports and facilitates aggregation for public health, quality management and other functions. The infrastructure facilitates transferring information to properly authorized end-point systems that aggregate data for such purposes.

5. **Federation:** To maintain the local autonomy of decentralization, a common set of policies, procedures, and standards to facilitate reliable, efficient sharing of health data among authorized users is required. These standards or practices spell out when patient information can be shared, which patient data can be shared and how the information can be used. That is, the participating members of the health network must belong to and comply with agreements of a federation. Federation, in this view, is a response to the organizational difficulties presented by the fact of decentralization. Formal federation with clear agreements allows participants to exchange information that the provider and patient have decided to exchange.

   Specifically, agreements must be established between the participants in a federation that address how the participants share health data to treat patients, who has access to a patient's record for treatment purposes, what information is accessible through the federation, what other uses of the data such as public health or research are permissible, how the federation will be governed, service level agreements, and a number of other issues.

   Because many providers will not be able or perhaps willing to provide the levels of service required to participate in a federation, they may have to contract with business associates (in the HIPAA sense) to store their data in a repository that will sustain these service levels. Small physician practices might, for example, choose to store their data in a database provided by their system vendor (GE Logician users can already opt to store their data in an anonymized database) or they might choose instead to store data with other physicians in a medical society sponsored database. Some source systems' external data sources, such as commercial labs, currently store their data on-line for a limited period of time. They would have to either create or contract for long term storage.

Rationale (Infrastructure)

In order to provide a majority of their benefits, clinical applications must interconnect with other clinical systems. The potential to avoid medical errors and drug interactions, to deliver real-time prompts and reminders at the point of care and directly to the patient or caregiver, and to improve the ability to conduct clinical research depend on a highly connected network of regional healthcare communities that exchange data between effectively used clinical systems such as EHRs.

Unless there is purposeful attention paid to infrastructure requirements at the local, regional and national level, it is unlikely that piecemeal technology adoption will result in the connected infrastructure necessary to realize the quality of care and economic efficiency gains promised by IT. The network requires a high degree of connectivity that arises from trust, safeguards for privacy and security and a strategy that minimizes risks of patient data misuse. With that said the approach must be voluntary and built on the premise of patient control and authorization.

Because our incremental approach is designed to leverage existing infrastructure it dictates that secure connectivity be built on the Internet and its communication protocols. Part of the function of the "Common Framework" is to select security standards for confidentiality, authentication, integrity and non-repudiation (CAIN). The "Common Framework" also addresses reliable authorization, a common set of standards and a minimum set of capabilities required to participate in the network.

It is certainly possible to create sufficiently secure connectivity over the Internet today, but current approaches to such secure connectivity require a person-intensive process to establish and maintain electronic trust between the communicating parties. As networks get larger, the burden of creating and maintaining electronic trust will become overwhelming. A single, consistent secure connectivity approach will simplify these connections by eliminating the need for negotiating a different approach for each partner.

While we believe that a reference implementation is critical, we don't believe that it can or should slow progress, particularly on the bottom up portions of the work. The first steps in the reference implementation will involve selecting candidate suites or profiles of standards. The implementation of these standards in the reference implementation will necessarily involve choices that eliminate some of the variability in the standards. However, these choices should not prevent organizations that are ready from moving ahead with implementations -- small changes may be required but major changes should not.

We believe these recommendations are important next steps to creating a health information infrastructure that is safe in terms of privacy, reliable, and does not overburden the systems it interconnects.

2. Accurate Linking of Health Records

> Linking of patient information for high quality care can and should be done *without a National Health ID*.

Most patients receive care from a number of healthcare providers in different locations. Privacy advocates have always agreed that patients will get better care at lower cost if providers can more easily retrieve medical records in the hands of other providers. The benefits of linking medical records electronically include more prompt and accurate diagnoses, more appropriate

treatment decisions, and the avoidance of adverse consequences such as those that may result from drug interactions or allergies.[1] Efficiencies can be achieved if prior test results can be quickly retrieved without having to wait for new tests to be run and analyzed. Major cost savings flow from not having to replicate tests and other costs savings are realized (and privacy risks are reduced) by not having to copy and transport paper records

In the past, however, there seemed to be no easy way to achieve the benefits of linking records without jeopardizing privacy and associated values. Previous proposals for a national health identifier have been a major source of contention in the privacy debates and a stumbling block to linking health records. One major concern was that any identifier created for healthcare purposes would become as ubiquitous as the Social Security Number, becoming the single national identifier for every purpose. If the health identifier became a key that could unlock many databases of sensitive information, it would make all personal data more vulnerable to abuse and misuse.

Yet, for progress to occur we cannot be asked to choose between our privacy and our health. The Connecting for Health Steering Group asked that any proposed solution offer major improvements in healthcare but also protect the privacy of patient information and offer patients control over their records.

Guiding Principles (Linking)

1. Any proposed solution must support the accurate, timely, private and secure handling and transmission of patient records.
2. Any proposed solution must increase the quality of care, the economic sustainability of the healthcare system, and the privacy of patient data.
3. Any proposed solution must create value for many different kinds of participants, including individual healthcare professionals and patients.

Rationale (Linking)

In examining the advantages and disadvantages of various ways to link health information, we concluded that a national health ID is unworkable in the near-term and would not provide the hoped-for benefits even if it could be implemented. It is important to note that the recommendations on decentralized systems for inter-enterprise information sharing are important companion concepts. The system we propose radically eliminates the two largest perceived privacy threats associated with the linking of health records: centralization and national IDs.

Implementation of any national health ID has several critical weaknesses:

1. The political culture of the US is not amenable to national identifiers. The risk of privacy spills is also a significant disadvantage if one identifier is the key to all of a person's health data.

2. A national health ID could not be implemented in a short period for two reasons. First, creating and implementing a process to issue a national health identifier would be

[1] According to the Institute of Medicine, more than 500,000 people are injured annually in the United States due to avoidable adverse drug events. See *To Err is Human, Building a Safer Health System* By Linda T. Kohn, Janet M. Corrigan, and Molla S. Donaldson, Editors. *Committee on Quality of Health Care in America, Institute of Medicine, National Academy Press*, Washington, D.C. (2000) Available at: <http://books.nap.edu/books/0309068371/html/index.html>.

expensive and require years. Second, current health IT systems don't support the easy addition of external, searchable identifiers. A new national identifier would require upgrade expenses for every institution in the U.S. healthcare system, and therefore create a significant lag in adoption.

3. Even if simple implementation were practical, the health ID would simply be another identifier, and would be subject to the same inaccuracies and distortions that have plagued any single identifier approach we currently have. (One major health IT network we surveyed estimates that there are transpositions and other errors in Social Security numbers up to 12 percent of the time.) In contrast, linking using multiple identifiers has been the subject of intense research and development over the years, and methods exist to achieve accurate linking up to 99.8 percent of the time.

To mitigate certain major privacy risks, the best protection is not to aggregate data. From a privacy perspective, the fundamental contribution of the Connecting for Health Working Group on Accurately Linking Health Information is to show that the benefits of information sharing can be achieved without any centralization of records and without unique national identifiers. Instead, the system contemplates a network of networks, linked only by directories of identifying information pointing to the sources of records. The directory system knows where records are, not what is in them.

Under the system we propose, decisions about linking and sharing are made at the edges of the network. The system supports (1) linking of records via a directory of pointers and sharing among healthcare providers participating in the system, but it also allows (2) linking without sharing, or sharing pursuant only to higher authorization, as well as (3) the ability to choose not to link information in certain treatment situations, such as drug or alcohol rehabilitation. The approach is based on the proposition that we should leave it to patients to determine locally with their providers what to link and what to disclose. By leaving these decisions at the edges, the architecture supports a range of approaches. It also allows higher levels of approval to be set locally for sharing some records.

Preserving these privacy options is important to ensuring acceptance of the system and its benefits. Trust is a crucial component of the doctor-patient relationship, including those elements of the relationship that involve the disclosure and sharing of sensitive information. Privacy is an important factor contributing to that trust. Privacy advocates have long agreed that patients should be informed by providers of the benefits of linking records. However, even well-informed patients are reluctant to share information because of privacy concerns. [2] Patients will be more likely to accept a scheme of automatic widespread sharing for healthcare purposes if they can choose, with assurance, to ensure that certain records will not be linked or disclosed. In this regard, the proxy for patient trust is often the primary care physician's trust: patients are likely to trust a system that their personal doctor trusts.

The full report of the Connecting for Health Working Group on Accurately Linking Health Information will detail this proposal and be made available later this summer.

[2] A 1999 survey by the California HealthCare Foundation showed that even when people understood the advantages that could result from linking their health records, a majority believed that the risks of lost privacy and discrimination outweighed the benefits.

3. Rate of Adoption of Clinical Applications

a. If funding and reimbursement incentives are provided to encourage the adoption of IT, they can include a wide range of applications from comprehensive EHRs, and incremental applications to simple data exchanges, provided these applications do not represent "dead ends".

b. Consider certification for EHR applications to assure that incentives result in the use of systems that meet a minimum set of functional capabilities using the HL-7 EHR functional standard and incorporate a minimum level of interoperability.

c. Represent all stakeholders in the governance of the certifying organization(s) and place minimal compliance burdens on care delivery organizations.

Guiding Principles (Applications)

1. Enable the Full Spectrum of Applications: The full EHR system, limited scope provider applications and specialized applications such as those that support reference laboratories will participate in the infrastructure.

2. There is a special need to facilitate the proliferation of EHR systems in order to engage more care providers in information-based collaboration.

3. Accept the Full Spectrum of Readiness: Accommodate diverse levels of readiness among providers.

4. Value-based Prioritization: Should choose candidate incremental applications by focusing on high-value use cases and exchange transactions

5. No Dead-Ends: Incremental approaches are necessary and valuable, as long as they are not dead-ends. The criteria include:
   a. Incremental steps must make adoption of the ultimate interoperable, standards-based EHR more likely, not create silos that do not integrate well.
   b. Should provide a clear migration path to a seamless end-user experience without loss of time and money investments previously made.
   c. Should utilize, and contribute to the building of, the "Common Framework," and not create an incompatible or competitive networking technology.

Rationale (Applications)

In order to provide a majority of their benefits, clinical applications must interconnect with other clinical systems. Electronic prescribing systems without data about the patient's weight or renal function provide much less benefit than when these data are available. Similarly, a health information exchange infrastructure without any applications to originate and receive data is entirely useless. We must avoid implementing EHRs or EHR components that preclude health information exchange.

The healthcare applications to be implemented, and the common health information infrastructure needed for interconnectivity, are highly interdependent. This may present a

dilemma about where to begin. Some would suggest focusing on incentives for EHR adoption as stand alone systems within provider enterprises, and trust that interconnectivity between them will emerge later. Others advocate constructing health data exchange networks first, assuming these will be a driver for the adoption of network-aware applications. Both of these extremes are to be avoided.

Focusing solely on accelerating adoption of local EHRs will continue the legacy that we have today—with proprietary, albeit more sophisticated, programs that cannot interoperate without a great deal of cost. Conversely, an isolated emphasis on infrastructure could leave us with an expensive network that lies unused, like the miles of "dark" fiber optic cable in the ground. Instead, our recommendation is that both applications and infrastructure should be developed and adopted simultaneously, in incremental steps that always bring us closer to the ultimate goal, and that deliver positive value for the adopters at every stage. Just as with the network, the incremental steps must follow a plan whereby each step is a move closer to the ideal.

Given the challenge of transitioning our incredibly complex $1.6 trillion healthcare industry from paper records to digital data, no one is seriously advocating an extreme "big bang" approach. But there are risks in an incremental approach as well, because isolated steps taken without an integrated strategy toward the long-term goal can lead to dead ends. There were many strong views about this area, with valuable observations on both sides. Some felt that implementing the full EHR was too disruptive and that most products are still at early evolutionary states, and cited current low penetration rates as proof. Others argued that a smorgasbord of isolated incremental applications would disrupt workflow, be difficult to learn and that without full EHR functionality, the safety and quality improvements from clinical decision support would never materialize.

Some participants pointed out that, readiness for IT varies widely among providers. Forcing "baby steps" on those who are fully ready for the jump to a full EHR is as counterproductive as expecting too big a leap from others. Therefore we designed our actions to accommodate this diversity of needs and readiness as well.

The Connecting for Health participants found several specific examples of incremental applications and data exchange that hold promise, including:

- Electronic Prescribing
- Electronic lab result reporting
- Electronic imaging reports
- Electronic disease registries
- Electronic medication management systems
- Continuity of Care Record data exchanges (if harmonized with HL7 standards)
- Electronic quality data submission
- Electronic symptom/disease surveillance for public health use cases
- Secure patient/physician email
- Administrative data exchange, e.g. eligibility, claims, remittance
- Clinical guideline prompts

However, these applications must be designed and implemented in such a way that the path toward the full EHR is clear and the likelihood of reaching that ultimate goal is increased, not decreased. For example, an electronic prescribing application should allow the user to add other functionality such as clinical documentation and decision support that move them toward the full EHR rather than requiring them to switch to a different product. Without this requirement, the

sunk costs in money, time and staff disruption and the difficulty of carrying data forward will continue to hurt the marketplace.

In the near term, these incremental applications represent nimble opportunities to change provider behavior, and to build out the necessary infrastructure. Many of these incremental opportunities achieve their quick return by providing service directly to patients and in so doing increase public interest and trust in health IT. Over the long term, these incremental applications must become seamlessly integrated functions within the EHR, and their networks must mesh smoothly with the complete health information infrastructure. Imminent funding for some of these incremental applications represents a significant opportunity if these requirements are served, and a significant threat if not.

4. Data Standards

a. Focus on implementing the "ready set" of standards that are mature and proven. Many of these standards have already been identified by the Consolidated Health Informatics initiative and Connecting for Health.
b. To ensure interoperability there is an immediate need for certifying interface conformance. The certification methodology should be developed in conjunction with the Reference Implementation.
c. Establish a certifying authority and appropriate, affordable and scalable interface conformance methods based on combinations of standards for specific information exchange needs that support differing levels of sophistication.
d. Fund some regional and local health information exchange initiatives to provide a test-bed for these interface standards.
e. Publicize and share the approaches to secure Internet transport in the Reference Implementation -- and facilitate a smooth transition to evolving standards that will make this problem more tractable for large networks.

Guiding Principles (Data Standards)

1. **Avoid "all or nothing" requirements.** Employ standards to work with high-function and lower-functioning systems and to facilitate the best possible interoperability among systems of differing levels of sophistication.

2. **Use nationally adopted standards in regional implementations**. The cost of conforming to standards will be spread over many more users if the manufacturers of information systems know that the code they develop will be used nationally. We assume minimal thresholds for participation in the system on the assumption that, by offering some value in return for some embrace of standards, we will be able to maximize early membership in such networks. Once in, the members will have both the incentive and opportunity to become increasingly standards-compliant, and therefore to have increasingly high levels of interaction with one another.

3. **Certification of interfaces is an important way to reduce the costs of building health information networks**. The few health information networks that now exist have been developed through a labor-intensive process of developing and testing interfaces. We can avoid replicating this expense for each new network through third-party, automated testing that uses automated methods to certify the conformance of an information system. Such certification must simultaneously apply

to the full profile of standards that work together to achieve interoperation. There is considerable work to do on the methodology and governance necessary to make interface certification function optimally and thereby achieve the economies of scale that derive from uniformity of interfaces at a national level.

Certification methodology must be developed as part of the "Reference Implementation." This is mandatory in order to ensure integrity of the standards, implementation guides, "Reference Implementation" and certification process.

Rationale (Data Standards)

The importance of the use of data standards in realizing our vision remains paramount. All the standards that are needed to get started exist today. The question is how to best apply them to specific use cases and how they should evolve over time. Near-term focus should be on getting the "ready set" of standards identified by Connecting for Health and by Consolidated Health Informatics implemented. Implementing these standards requires profiles, certification (see below) and implementation in applications. We recognize there are many standards that are necessary for complete interoperability and none that are by them selves sufficient. These standards come from different organizations such as the Internet Engineering Task Force, World Wide Web Consortium, X12, HL7, NCPDP and the College of American Pathologists and serve different functions. Some are specific to healthcare while others are applicable across all industries. They must be combined in a coordinated fashion. These combinations or profiles of standards define a suite of standards that we need to fulfill the needs of a specific use case. Once developers implement the suite of standards within an application they must be certified to ensure that they will interoperate seamlessly.

For example, The Medicare Modernization Act (MMA) requires a suite or profile of standards to be chosen and specified sufficiently to address the use case. The MMA directs HHS to recommend standards required to support electronic prescribing. This profile will almost certainly contain the Internet and IP at the lower levels, NCPDP messages for data transfer at a higher level and RxNORM for content. Like most messaging standards, NCPDP provides a degree of flexibility and HHS will have to create implementation guides that eliminate most of this flexibility in order to create seamless interoperability. The lower level standards will have to be the same for all new initiatives in order to avoid dead ends.

When adopting clinical information standards there is an important trade-off between specifying a requirement that the data be minutely structured and coded, on the one hand, or allowing it to be represented as simple text, suitable for interpretation by a person. The former approach is required for computer decision support, abstracting for public health surveillance, or aggregation for research and quality determination. The latter approach is important in the short term because it minimize the burden on users.

Certification of interfaces must therefore be based on use cases that involve interoperation of systems with different levels of sophistication with respect to handling structured data. They should consider the benefits of the HL7 Clinical Document Architecture for sending information in a mixed format (both structured and unstructured) useful both to unsophisticated systems and sophisticated ones.

If we create the methodological groundwork for interface certification, there is considerable opportunity to achieve this certification over the Internet without labor-intensive on-site testing. Organizations that fund regional health information projects should foment a collaboration between the National Institute of Standards and Technology, the standards development

organizations, major IT vendors and healthcare information trade organizations to establish the methodology, and then use it on the early projects. The experience gained in immediate projects will inform the eventual establishment of a public/private consortium to provide interface certification.

Standards-development will be a continuing process. As policymakers, providers, and vendors anticipate increased use of health IT by patients and families, and increasing patient self-care using information tools, data standards suitable to transmittal of patient-sourced information will be necessary. Some current standards work – such as the HL7 EHR functional model – contain most of the functionality needed by the PHR. Standards organizations should give greater attention to including codes and vocabularies for such information as symptom, behavior, functional, and adherence reporting as well as the need for patients to easily and uniformly interpret the presentation of EHR data that is now becoming available to them.

The preceding recommendations represent the combined efforts of members of the Technical Panel and the Working Group on Accurately Linking Health Information.

Connecting for Health
Technical Panel

Mark Leavitt, MD, PhD, FHIMSS, Medical Director and Director of Ambulatory Care, Health Care Information and Management Systems Society
J. Marc Overhage, MD, PhD, (Co-Chair), Associate Professor of Medicine, Indiana University of Medicine Senior Investigator, Regenstrief Institute
Wes Rishel, (Co-Chair),Vice President, Gartner Research, Chair Emeritus HL-7
Clay Shirky, Adjunct Professor, NYU Interactive Telecommunications Program, Chair, Working Group on Accurately Linking Health Information
Paul Tang, MD, Chief Medical Information Officer, Palo Alto Medical Foundation

Connecting for Health
Working Group on Accurately Linking Health Information

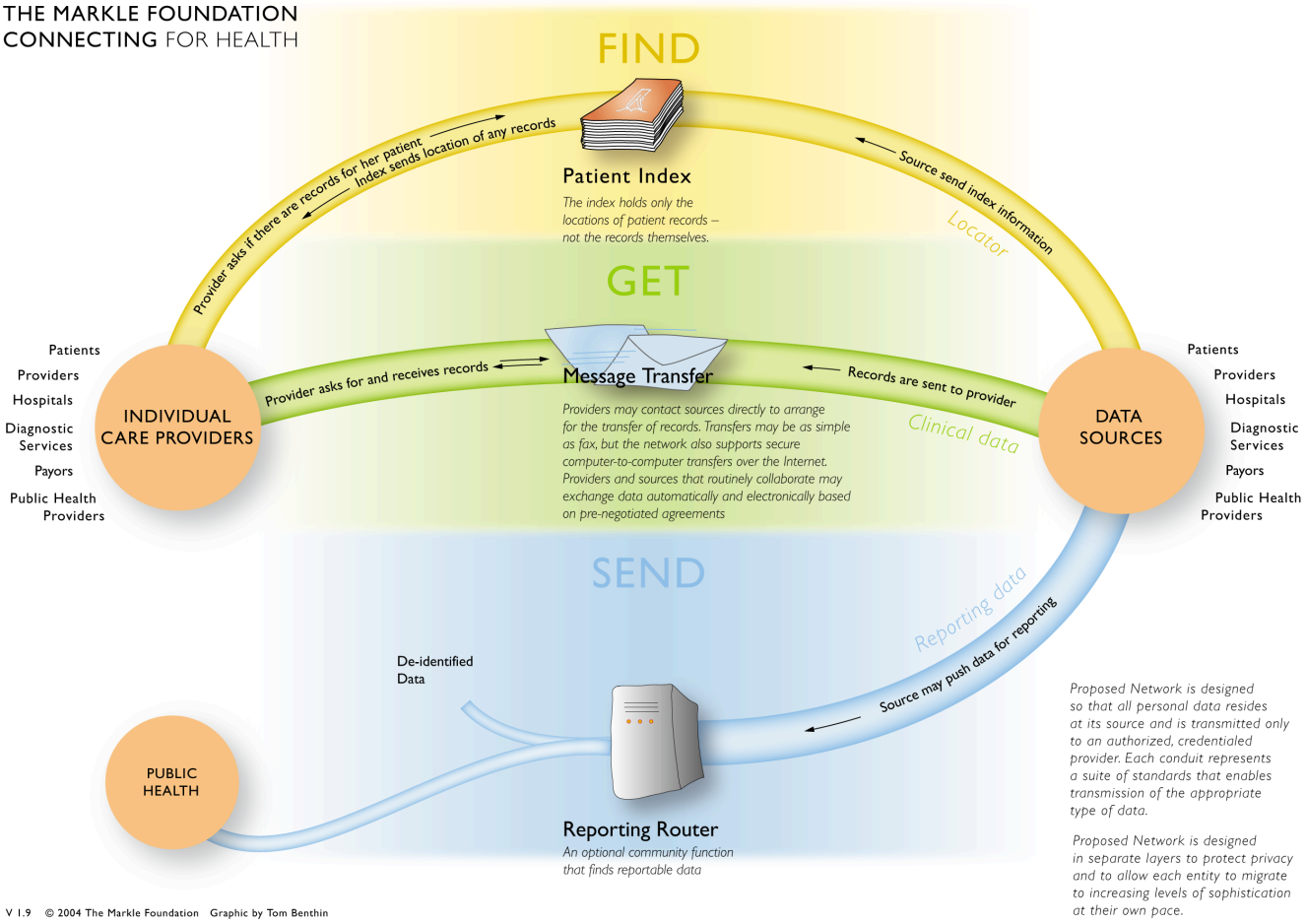
R. Steven Adams, President & CEO, Founder, Reach My Doctor
David Bates, MD, MSC, Medical Director, Clinical and Quality Analysis, Partners HealthCare System, Inc. and Professor of Medicine, Harvard Medical School
William Braithwaite, MD, PhD, Health Information Policy Consultant
Jim Dempsey, Executive Director, Center for Democracy & Technology
Daniel Emig, Director, Technology Marketing, Siemens Medical Systems
Lorraine Fernandes, Senior Vice President, Initiate Systems Healthcare Practice
Mike Fitzsmaurice, Senior Science Advisor for Information Technology, Agency for Healthcare Research and Quality
Paul Friedrichs, PKI Chief Engineer, Defense Information Systems Agency
Janlori Goldman, JD, Director, Health Privacy Project
Gail Graham, RHIA Director, Department of Veterans Affairs
John Halamka, MD, Chief Information Officer, CareGroup Healthcare System; Chief Information Officer, Harvard Medical School
W. Edward Hammond, PhD, Professor, Community and Family Medicine Duke University
Jeff Jonas, Founder and Chief Scientist, SRD; Member, Markle Foundation Taskforce on National Security in the Information Age
Stephanie Keller-Bottom, Director, Nokia Innovent Ventures
J. Marc Overhage, MD, PhD, Associate Professor of Medicine, Indiana University of Medicine Senior Investigator, Regenstrief Institute, Co-Chair, Technical Panel
Ben Reis, PhD, (Working Group Staff and Markle Foundation Program Manager)
Clay Shriky, (Chair), Adjunct Professor, NYU Interactive Telecommunications Program
Peter P. Swire, JD, Moritz College of Law, Ohio State University John Glenn Scholar in Public Policy Research Formerly, Chief Counselor for Privacy in the U.S. Office of Management and Budget
Paul Tang, MD, Chief Medical Information Officer, Palo Alto Medical Foundation
David Weinberger, Publisher, Journal of the Hyperlinked Organization

We are grateful to these additional experts who made significant contributions at different points in the process:

Jared Adair, Computer Sciences Corporation
William Braithwaite, MD, Independent Consultant
W. Edward Hammond, PhD, Professor, Community and Family Medicine Duke University
Donald Mon, PhD, Vice President, Practice Leadership, American Health Information Management Association
William Rollow, MD, Deputy Director, Quality Improvement Group Office of Clinical Standards and Quality Centers for Medicare and Medicaid Services
William Yasnoff, MD, PHD Office of the National Coordinator for Information Technology

PROPOSED NETWORK

THE MARKLE FOUNDATION
CONNECTING FOR HEALTH



Proposed Network is designed so that all personal data resides at its source and is transmitted only to an authorized, credentialed provider. Each conduit represents a suite of standards that enables transmission of the appropriate type of data.

Proposed Network is designed in separate layers to protect privacy and to allow each entity to migrate to increasing levels of sophistication at their own pace.

CONNECTING FOR HEALTH[SM]

MARKLE FOUNDATION *A Public-Private Collaborative*

Connecting for Health is an unprecedented collaborative of over 100 public and private stakeholders designed to address the barriers to electronic connectivity in healthcare. It is operated by the Markle Foundation and receives additional support from The Robert Wood Johnson Foundation. Connecting for Health is committed to accelerating actions on a national basis to tackle the technical, financial and policy challenges of bringing healthcare into the information age. Connecting for Health has demonstrated that blending together the knowledge and experience of the public and private sectors can provide a formula for progress, not paralysis. Early in its inception, Connecting for Health convened a remarkable group of government, industry and healthcare leaders that led the national debate on electronic clinical data standards. The group drove consensus on the adoption of an initial set of standards, developed case studies on privacy and security and helped define the electronic personal health record.

For more information, see www.connectingforhealth.org.