Exchanging Health Information: Local Distribution, National Coordination

As more communities develop information-sharing networks, a coordinated approach is essential for linking these networks.

by John Halamka, J. Marc Overhage, Lygeia Ricciardi, Wes Rishel, Clay Shirky, and Carol Diamond

ABSTRACT: The fragmentation of our health care system, our need to accommodate the diversity of existing health information exchanges, the lack of consistent implementation of clinical information standards, and the need to protect patients' privacy and maintain trust are all challenges to overcome in achieving broad-scale interoperable health information exchange. We propose several steps to coordinate information sharing among regional and other networks through universal adherence to a basic framework of policies and standards. The critical policy action is the identification of a "common framework" of standards and policies, maintained by a new Standards and Policy Entity that reflects both public- and private-sector participation.

INFORMATION TECHNOLOGY CAN BE A KEY to meeting the diverse needs of patients and providers in a health care environment burdened by rising costs, inefficiency, preventable errors, and poor quality of care. Although there is general agreement that the strategic application of information technology (IT) could mitigate these problems, there is less agreement on how the United States should organize an infrastructure for implementing interoperable IT.

Participants in the U.S. health care system face the need to exchange personal health information at three levels: among patients and providers within an enterprise, across a community, and across the country. Although adoption of electronic health records (EHRs) in the United States has been slow, organizations...
that have introduced them have often instituted local approaches to facilitate information exchange among components of their organizations—between the pharmacy and nursing unit or between the lab and physician’s office, for example.

Several communities have begun working on regional information exchanges, in which multiple, sometimes competing, organizations agree on systems for sharing patient information. Prominent examples include Santa Barbara, California; the Indianapolis region; and greater Boston, Massachusetts. Local leaders have convened the parties and developed home-grown technical solutions to the many challenges of data standardization and common privacy and security policies.

Yet there are no clear ways for health information exchange to expand easily beyond these initial projects, other than within coherent enterprises, such as the Veterans Health Administration (VHA) network. When a patient from New York enters an emergency room in San Diego, there is no possibility of quickly retrieving the relevant information about the patient’s history, recent lab tests, allergies, or medications. When people relocate to a new community, their entire medical history is typically lost. The fragmentation and lack of uniformity across the country also prevents the aggregation of public health, quality measurement, or research data in any efficient or standardized fashion.

Planning for a health information network that will accommodate patient care needs across a fragmented delivery system must begin with an acceptance of the structural and political realities of the moment. Energetic leaders are investing time and money in IT solutions at the provider and community levels, yet they now work without a framework that would allow these innovative systems to communicate with each other. We face the possibility that hundreds of well-intentioned—and even locally successful—information networks will never be able to exchange information with each other. This paper proposes an approach to creating a health information infrastructure that supports continuous, expanding, and uniform exchange of information throughout the United States.

Identifying The Challenges

Several difficult challenges exist to the creation of a uniform health information infrastructure on a national scale.

- **Consistent standards.** Although a core set of data standards is generally recognized, and most vendors can implement these standards in their systems, they are not consistently implemented between every pair of institutions that wish to exchange data. In addition, most “real-world” problems, such as transferring a prescription electronically, require that several sets of standards be bundled together: some for the underlying demographic or clinical data, some for packaging the message, some for the transmission. These “profiles” of standards have not been identified, documented, or commonly adopted.

- **Privacy and security.** Information exchange rests upon trust—each network user trusts that every other user will handle sensitive information in a predictable
way. Other than the minimal requirements of the Health Insurance Portability and Accountability Act (HIPAA) of 1996, there are no uniform agreements about security or privacy of health information across a network.

Consumers and patients are fearful of uses of their personal health information by anyone other than their doctor. The public is legitimately concerned: Institutions may repair mistakes in financial transactions through economic adjustments, but privacy breaches involving health information can be both extremely hurtful and nearly impossible to undo. Without widespread trust in health information exchange, patients might not tolerate increased electronic information sharing among providers, payers, researchers, or others.

- **Pluralism.** A national approach to interoperability must be pluralistic. Interoperable networks such as the Kaiser Permanente system and the VHA exist on a national scale. There are also substantial local and enterprise IT networks, such as those operating within the Partners HealthCare System (Boston), or the Indiana Network for Patient Care. Any approach to interoperability to support information exchange among these existing systems must accommodate all of these local systems and allow newcomers of every level of sophistication to participate.

### Addressing The Challenges

Connecting for Health, a large, multistakeholder collaborative, has developed an approach to widescale health information exchange that addresses these challenges. The Connecting for Health approach reflects the participation of the principal interest groups in U.S. health care and represents an unusual consensus of views on a practical implementation path. We believe that general adoption of a formal set of technical components, standardized methodologies, and explicit policies for use and governance can permit rapid attainment of an interoperable health information environment that supports modern health care practice. We call this bundle of standards and policies the Connecting for Health Common Framework for information exchange.

Broadly, health information exchange is likely to consist of many networks that are capable of communicating and exchanging information with each other. Some networks will be geographically defined (so-called regional health information organizations, or RHIOs); others will be defined by affinity groups of various kinds—networks of cancer research centers, collaborating businesses, or distributed enterprises. Internally, these networks may take a variety of approaches to governance, data standards, data management, financing, and privacy policies. But to achieve national interoperability, every geographic or affinity-based network must adopt the standards and policies that the Common Framework comprises.

A decentralized and federated model for health information exchange will help protect the privacy and security of information while allowing accurate and timely access to information, as long as all participants adhere to a minimum set of uniform standards and policies. Personal health information will remain where it
is today: in the hands of doctors, hospitals, and others who provide care to patients. All of those who generate health information for patients are its stewards. Patients must ultimately be able to control the access to and use of their personal health information in partnership with their providers. Over time, more and more of these data will be stored and transmitted using uniform standards.

This model recognizes the profound fragmentation of the U.S. health care system. Many types of institutions are part of the current system, from giant hospital systems to individual practices, with all manner of specialists, clinics, and agencies in between. The Common Framework will facilitate the transfer of selected information from one endpoint system to another, as is required for providing care and supporting informed patient participation. It also supports and facilitates authorized aggregation for public health, quality management, and other functions. The decentralized approach obviates the need for storing identifiable data in a central database but takes advantage of existing aggregates of data where available or necessary.

Accuracy in identifying both a patient and his or her records with little tolerance for error is an essential element of the Common Framework. Each network that participates in information exchange must maintain an index of patient records that tells authorized requesters where a patient's information is stored without disclosing what those files contain. To assure interoperability between regions and other networks, these indices must follow common standards for coding patients’ demographic information. In the absence of a unique identification number, patient matching will occur using algorithms (as are now used by most large database indices), and every network index will need to accommodate the same formats for receiving and replying to demographic queries.

The system as a whole, and each component of it, must be reliable—able to assure a uniform, minimum level of system service quality in addition to backup mechanisms, so that stakeholders can count on the availability of the overall system. It must provide for near-real-time information access, not only for routine clinician and patient needs but also for particularly time-sensitive specialties such as emergency medicine and the monitoring of disease outbreaks, bioterrorism, or contamination of the food supply.

The Common Framework For Information Exchange

This approach—premised on privacy and patient control and built on decentralization, federation, and reliability—can only work if all participants conform to a Common Framework, which consists of the essential technical and policy requirements to enable the interoperability of standard interfaces and transactions at the local, regional, and national levels. The technical standards address secure transport over the Internet and other networks, and they provide the essential components required for the infrastructure, including secure connectivity, reliable authentication, and a suite of defined interchange formats for health care
IMPLEMENTATION

data. The policy standards address the privacy, use, and access policies for the exchange of health information. The Common Framework also provides a uniform methodology for the identification of users. The suite of interoperability standards will expand and be enhanced over time.

The Common Framework is the basis of all of the desired uses or applications—from e-prescribing to public health surveillance—that require specific, uniform interoperable standards to support information exchange. Use cases and accompanying information standards will be specified for each of the applications of the network and will be supported by detailed implementation guides. The participants in regional and other networks will determine which profiles are appropriate to address the requirements established by their stakeholders.

This approach to interoperability is premised on a model of patient authorization and control. Patients must be able to choose whether or not to participate in sharing personally identifiable information; exercise their rights under HIPAA; control who has access to their records (whether in whole or in part); see who has accessed their information; review, contribute to, and amend their records (without unreasonable fees); receive paper or electronic copies of their information; and reliably and securely share all or portions of their records among institutions. Once patient consent has been granted for access to a certain type of information, however, patients should be able to access it freely.

**Flexibility.** This approach is flexible in several ways. First, it is heterogeneous with regard to the types of technology and the functions of the various networks and other entities that use it, as long as all of them adhere to the Common Framework. This enables users of varying levels of technical and functional sophistication to use it for a variety of processes, and it acknowledges the heterogeneity of existing systems. Second, it is flexible in that it facilitates communication among endpoint systems at varying levels of sophistication in the structured and coded representation of data and supports the evolution of systems in this regard. For example, while some might use the system to locate records and request them by telephone, others may draw on it to support the full electronic exchange of highly structured data for sophisticated data analysis and decision support. This flexibility is necessary because health information will continue to be a mix of unstructured, structured, and coded data. The Common Framework provides standards and procedures that allow two systems that support highly coded data to exchange them without loss of data, while also allowing a system that supports little coding to send and receive information from similar and more highly structured systems. Lastly, this network design can evolve over time to address the changing needs of users and to increase in scale as the numbers of users and their transactions grow; it supports a reasonable level of variation and innovation in response to local needs.

**Incremental changes.** We recognize that any attempt to change the U.S. health care system faces major constraints. Although the challenges facing this system would warrant a full-scale “moonshot” approach, the system’s complexity, di-
"The interoperable system should be coordinated and built on a plan that recognizes the need for a learning curve."

versity, and distributed nature suggest that an approach that builds on and integrates existing networks is more likely to succeed. Furthermore, the standards, validation mechanisms, and governance structures cannot spring into existence at once. The interoperable health information system should be coordinated and built on a plan that recognizes the need for a learning curve. The lessons learned from developing harbinger regional or other networks can prove and improve approaches, leading to accelerated replication and success based on early experience.

- **Regionalized approach.** This approach is not based upon a national central repository of patient information or a mandated national patient identifier. Instead, it is a pathway that facilitates, with appropriate authorization, private and secure information identification and access among regional and other networks. Health information resides with the providers that generate it or with patients themselves. Health care applications or endpoint systems (such as EHRs) conform to the Common Framework and are important extensions of it, but not strictly part of it.

- **Lowering of barriers.** This model of interoperability also minimizes any additional financial or technical barriers (other than the requirement to comply with the Common Framework) to information sharing for patient care. Any appropriate and authorized organization or person can participate in the network without sizable economic barriers and can participate at almost any level of technical sophistication. The underlying infrastructure is not a proprietary network that is owned and operated by particular stakeholder groups.

- **Other benefits.** In addition to being practical, this incremental and decentralized approach to electronic connectivity provides other benefits. For instance, it greatly reduces the risk of data misuse, since the information is not in a single database. Judgments about who should have access to patients' information remain under the control of patients and the clinicians and institutions that are directly responsible for their care. Once data are centralized, we have to rely solely on policy to protect the data; a decentralized approach allows the data holders to exercise control as well.

To meet the needs of clinical research, public health, and quality measurement, the Common Framework also supports aggregation of data for patients from across the health care environment. By standardizing the interfaces and creating common policies, communities will be capable of aggregating data for population-based uses, subject to appropriate deidentification or legal requirements. In addition, researchers have developed methods that will allow anonymous aggregation of data across systems that support common interfaces.

We do not envision that coordination will require the replacement of existing software systems. Most existing EHR systems are capable of conforming to the
technical standards and others can be connected through "middleware" technologies, which wrap standard-based interfaces around systems. Newly deployed hardware and software will likewise be able to interoperate with legacy systems if they conform to the Common Framework.

The Need for A Standards And Policy Entity

The Common Framework, and the trust and interoperability it enables, will come about only if an entity with sufficient authority and influence is responsible for its specification and perpetuation, creating the confidence that is critical to adoption. As we envision it, the Standards and Policy Entity (SPE) would be a public-private collaborative body that would identify and specify the detailed implementation rules, including business rules, for the policies and standards that make up the Common Framework. In collaboration with existing standards-development organizations (SDOs), and drawing on their work, rather than creating new standards, it would identify and recommend only the information policies and technical standards essential for establishing privacy, security, and interoperability, and would also be responsible for their interpretation and dissemination. Although the foundational elements of the Common Framework can be specified early on, the identification of guidelines for the full portfolio of health information needs will take many years to develop, and guidelines must continue to evolve along with technology. The SPE would therefore need to establish priorities among competing demands for its attention.

In addition to performing the functions described, the SPE would support provider and institutional adherence to its guidelines in ways that the history of network development shows to be important. For example, once an integrated suite of standards was chosen and associated policies developed, the SPE would have to promulgate detailed implementation guides for specific situations (for example, how to send a prescription from a doctor to a pharmacy electronically) to help users "connect the dots" between the status quo and the desired outcomes.

Although we do not propose a detailed blueprint for the SPE, we propose several guidelines to drive its creation.

Mission and functions. The SPE would be responsible for identifying, specifying, interpreting, and disseminating the policies and bundles of standards necessary for the sharing of electronic health information. Relevant policies include agreements associated with privacy; security; methods for the accurate identification of patients, professionals, and institutions; and baseline rules for user authorization and use and access policies. Standards that would fall within the SPE's purview include those for message transport, privacy and security, and data standards. These policies and standards collectively make up the Common Framework, which will maintain a consistent core but evolve to meet the developing needs of the health sector and the changing technologies it employs. For example, the SPE might endorse a particular approach to distributed identity management that would drive specific
standards and policy choices.

The SPE would identify priority situations (such as tracking all of a particular patient's medications and assuring that they are compatible), and suites of standards, based on the input from many stakeholders. It would also develop detailed technical specifications for implementing those standards.

The purpose of the SPE must be clearly defined, and its activities must remain tightly constrained to those for which it is designed. Failure to do so could result in an unintended accretion of duties and thus diminish the SPE’s credibility and effectiveness as a focused policy and standards entity.

- **The importance of coordinating policy and standards functions.** Seemingly narrow technical choices and standard-setting processes can have a broad and lasting impact on public policy and individual rights and can affect the overall cost and feasibility of implementing electronic connectivity in health care. The recent ChoicePoint privacy spill and the proliferation of unsolicited commercial e-mail on the Internet exemplify such reactive and often “too little too late” attempts at policy patchwork solutions. To avoid such pitfalls and to achieve maximum policy and technical consistency, the SPE should be the sole entity responsible for both the policy and technical components of the Common Framework.

- **Structure.** The SPE could be a government function, an independent public/private partnership, or a private organization. Regardless of its corporate structure, however, it is clear that it must allow the diverse members of the health care community, including representatives of the public, to debate and determine policy and technical guidelines related to health information sharing.

The SPE must be able to act on issues of interest to its constituents without accepting the lowest-common-denominator consensus. To do so it must have (1) a well-defined mission and structure, including an independent board of trustees, a secure source of funding, and a strong executive office; (2) policy procedures that enable all interested parties to debate in an open and transparent way; (3) the ability to resolve disputes through an open and transparent process; and (4) a mechanism to adopt and validate its standards.

- **Broad stakeholder representation in governance.** The SPE’s activities will affect a great variety of interest groups, including IT vendors, providers, payers, and the public—for example, through the accelerated availability of interoperable EHRs. The policies and standards it develops will ultimately facilitate or impede adoption of personal health records and other patient-focused tools. The representation and consultation structure of the SPE must therefore create a meaningful role for affected groups, including the public, in its operation and policy development.

- **Accountability, transparency, and trust.** The SPE can succeed only if it remains accountable to key stakeholders. Its bylaws must include effective procedures for independent review of controversial decisions, and its reporting arrangements—most appropriately to Congress and other parts of government—must be clear.

The importance of transparency in the SPE’s governance is especially great be-
cause of its unique relationship with its stakeholders—a relationship based more on trust than on financial, legal, or political ties. As our collaborators in Connecting for Health have emphasized, generating the trust necessary for data sharing is far more difficult than solving the associated technological challenges.

- **Building on existing work.** Although the SPE's primary obligations would be to its stakeholders and member organizations, its authority and efficacy would depend heavily on the extent to which it can collaborate effectively with existing SDOs and other relevant entities. Many of the SPE's policy and technical efforts would build on existing efforts; there would be no reason for it to replicate work already done by others. Evidence that these groups have accepted the SPE's authority, and resolution of doubts or concerns they may have about it, would be a measure of the SPE's success.

- **Support for evolution and innovation.** Although the SPE would not be directly responsible for promoting the development of an interoperable health system beyond the narrow scope of its coordination activities, it could support and preserve the long-term evolution and innovation of the health sector instead of hindering it.

**The Urgency Of Action**

More than 100 communities across the country are actively engaged in creating health information exchanges. Pharmacies and pharmacy benefit managers (PBMs) are offering medication management tools, chronic disease tools are being optimized for people with congestive heart failure or diabetes, and secure e-mail and result-reporting systems are being integrated with both inpatient and outpatient EHRs.

In a general sense, these developments represent positive movement toward the ideal future we envision. At the same time, however, this burgeoning of disjointed efforts could undermine achievement of our national goals: There is no guarantee that these initiatives will be compatible, either technically interoperable or following consistent and predictable policies for information handling.

This new health information environment—based on open, consensus-driven, and nonproprietary standards; uniform policies that protect privacy, assure security, and support existing trust relationships; and a common technical approach to linking personal health information—can be the springboard to a generation of innovation and improvement in health care and in personal health. Clinical models, self-care and decision-support tools, application and communications software, and even redesigned care practices will emerge within this new environment. Research and innovative approaches to prevention and treatment can be strengthened and the results integrated more rapidly into health care and health-related decision making. The delivery of high-quality care can become more likely, less expensive, and more timely if the right skills and knowledge can be brought to the right person at the right time. We can put patients and families at the very center of the health care system, supported and surrounded by an information envi-
ronment that they can use—or allow others to use—to make decisions, monitor health, provide feedback, and support strategic analytic functions that produce measurable improvements in health.

The authors acknowledge the substantial contributions to this paper by David Lansky and Stefaan Verhulst of the Markle Foundation.

NOTES


2. Recent studies emphasize that technology alone is not sufficient to address quality and efficiency problems; implementation and support are vital. See, for example, R. Koppel et al., "Role of Computerized Physician Order Entry Systems in Facilitating Medication Errors," *Journal of the American Medical Association* 293, no. 10 (2005): 1197–1203.


7. The implications of these differing degrees of interoperability are detailed in Walker et al., "The Value of Health Care Information."


