CONNECTING FOR HEALTH... a Public-Private Collaborative

CONNECTING FOR HEALTH

DECISION-MAKING FOR POPULATION HEALTH

"FIRST PRINCIPLES"

A Framework for Informed, Intelligent and Safe Decision-Making for Health in the 21st Century

Our Goal:

A health information environment that enables high-quality decision-making.

Preface:

Connecting for Health has proposed a nationwide framework for a secure "network of networks" to enable the sharing of personal health information where and when it is needed for the care of individual patients. This same environment must also support critical needs to evaluate and improve health care and the health of the general population. In the 21st century, the United States must have an information-sharing environment that enables each person to generate knowledge and make better health and health care decisions by analyzing data from disparate sources. This approach must be based on principles that support the efficient exchange of accurate information as well as the protection of individual privacy and personal choice.

Below is a draft of First Principles for Population Health Data Sharing and Decision Making. Derived from extensive discussions by the Connecting for Health Steering Group, these principles extend upon the foundation work of the Connecting for Health Common Framework (2006)[1] and the Roadmap on Achieving Electronic Connectivity (2004).[2]

First Principles:

1. Designed for Decisions

A 21st century health information environment will focus on improving the decision-making ability of the many actors in the health sector. Information technology provides value to health and health care by bringing timely, accurate, and appropriate information to a decision-maker at the right time and in the right way. Data collection alone does not lead to better decisions – indeed, too much or poorly organized data can distract us from filtering up to the most useful information upon which to base a given decision.

2. Designed for Many

A 21st century health information environment should empower a rich variety of users. The network can feed analytic tools in many settings and provide value to millions of

---

[1] Available online at: http://www.connectingforhealth.org/commonframework/

[2] Available online at: http://www.connectingforhealth.org/resources/cfh_aech_roadmap_072004.pdf

users – to consumers, families, health professionals, policy makers, public health officials, scientific investigators, and many others. The technical and policy framework for the network should anticipate the diverse requirements of this array of users – much like the Internet itself.

3. Shaped by Public Policy Goals and Values

A 21st century health information environment should achieve society's goals and values – such as to improve the health of individuals; to make the care delivery system more effective, safe, and efficient; to reduce and manage threats to public health; to respect confidentiality; and to increase scientific knowledge. The network serves both the personal care setting and public needs and values. It is obliged to respect and further public values such as individuals' ability to control the use of their information. Such policy and public values must be made explicit and subjected to public discussion, and then architected into the technology at the outset.

4. Boldly Led, Broadly Implemented

A 21st century health information environment should be guided both by bold leadership and strong user participation. The network's value expands dramatically with the number of needs it can meet and the number of participants it can satisfy. The network is not bound, for example, by a hospital's walls or the parameters of a research grant. A forward-looking generation of health care leaders will know that they are not building information systems to keep data from competitors or to deprive others of the opportunity for insight, but that they are contributing to a diverse, flexible, and expansive body of knowledge. Value will be created by those who are most skilled at accessing the right information, applying the right intelligence, and solving the right problems. New health care leaders must come together with a common vision to develop an architecture and policy framework that facilitates this kind of information environment.

5. Possible, Responsive, and Effective

A 21st century health information environment should grow through realistic steps. Overly complex or ambitious technology can exacerbate the problems we face, or introduce new ones. It is therefore essential to seek realistic steps towards the ultimate vision of a responsive, nimble system to enhance decision-making.

6. Distributed but Queriable

A 21st century health information environment should be comprised of a large network of distributed data sources. It should be possible to query across all of these sources without needing a central structure. We must avoid replicating (or even exacerbating) the current problem of uncoordinated health data silos, which result from duplicative efforts to build repositories and analytic systems, often drawn from the same data sources. We must also avoid the temptation to create a single repository of health information for each population health purpose.

7. Trusted through Safeguards and Transparency

A 21st century health information environment should earn and keep the trust of the public through policies that provide safeguards and transparency. Americans will support sharing their sensitive health information across the Internet if they trust in the security, privacy, and appropriate uses of the network. Such trust can be established through a combination of safeguards (including both technical and non-technical approaches) and transparency (of both decision-making process and practice). The technical architecture will allow

for tools to protect data against break-ins and theft, to provide anonymization, and to prevent data corruption or errors. The policy architecture will develop clear rules and guidelines through an inclusive and transparent ongoing process.

8. Layers of Protection

The 21st century health information environment should protect patient confidentiality by emphasizing the easy movement of queries and responses, rather than of raw data. The level of protection should be scaled to the risks, with identifiable data subject to the highest levels of protections. Many classes of authorized users should be able to send standardized queries across the network, allowing appropriate data sources to respond with aggregated or anonymized "answers" without compromising personally identifiable data. When requirements for additional identifiers are appropriate, additional levels of protections should be applied.

9. Accountability and Enforcement of Good Network Citizenship

A 21st century health information environment should encourage and enforce good network citizenship by all participants. Health sector leaders should take steps to increase the appropriate movement of health information and discourage those who pursue unauthorized uses. To receive public funding or to be welcome in various information exchange initiatives, participants must abide by both the technical and policy rules that permit the larger national network to function. The data-sharing infrastructure must include accountability and strong mechanisms for policy enforcement, auditing of data uses, assignment of liability for data misuse, and mechanisms for redress.