Designing the National Health Information Network

Patient and Consumer-focused Principles

January 18, 2005

Modern health care depends upon accurate, timely, understandable, and relevant information. Complete and useful information needs to be in the hands of patients, families, professionals, and health system managers to improve individual health, the performance of the health care system, and the nation's well-being. A properly planned information environment may achieve these functions without central databases, or new physical networks, or new entities. Though referring to a "network", the principles presented here describe the essential attributes of <u>any</u> approach to improving information connectivity in health care.

Information access and control

- People must have the ability to control who has access to their personal health information over an electronic health network - either directly or through the action of a designated proxy [or by choosing not to exercise that control]. This control can be exercised in whole or only with regard to selected elements of their personal health information.

- At a minimum, the structure and rules of health information networks must facilitate the ability of people to exercise their personal health information rights under the federal privacy regulation mandated by the Health Insurance Portability and Accountability Act (HIPAA).

- If people fear inappropriate disclosure and do not trust an electronic network, they may become less willing to seek care or provide consent to share even that information to which they otherwise would allow access.

- People should have the ability to review who has had access to their personal health information. Each individual or entity accessing personal health information over the network should possess a unique digital signature, through which patients can have access to a standardized profile of the entity or individual reviewing their PHI.

- No personal health information should be available to a provider or health professional that is not also available to the person it describes (with exception for cases of danger to the patient).

- People must be able to supplement or annotate their personal health information.

- Unreasonable or unaffordable fees should not impair the ability of each person to access, review or supplement their personal health information on the NHIN.

- People must be able to request correction of their personal health information and receive a timely response to the request.

- The NHIN must provide a sound method for allowing secure access and authenticating individual patient users that does not require physician or institutional mediation.

- People must have the ability to designate (and withdraw designation from) proxies who have full authority to manage their personal health information on the network.

- People must be able to choose whether or not their information is shared across the network – in whole or in part - at any time, without coercion or pressure.

Disclosure and accountability

- Before a provider initiates a transfer of personal health information through the exchange, affected individuals should fully understand the policies in place and the possible uses of that information. (First-time disclosure is sufficient for subsequent transactions.)

- Information elements central to network functioning, such as identifiers, authorizations and permissions, access histories, and index entries, must be presented in easily understood terms and formats to patients, consumers, and other authorized users for their review and possible correction or control.

- People should be informed of the ways their information may be used and must be able to choose whether to make their personal health data available for such use in various systems.

- Communications with people about the uses of and policies affecting their electronic health information must be conducted in simple, easily understood language.

- States should adopt common operating standards for data security and patient privacy protection, including established clearly described penalties for violations not covered by HIPAA (such as identity theft), and an accountable means for monitoring and prosecution of violations.

- People must be able to receive complete paper copies of any of their information available across the national network.

Functionality

- The NHIN must provide the capability for people to reliably and securely move all or portions of their personal health information from one health care entity to another.

- The NHIN should permit the aggregation of data (without patient identifiers) in support of quality measurement, provider and institutional performance assessment, prescription drug monitoring, patient safety, public health and other public interest objectives.

- Non-identifiable data sets generated from the NHIN should not be used for insurance underwriting or other commercial applications intended to provide preferential pricing or services to one group over another. Preferential pricing would not include differential payment to providers in recognition of quality performance.

- Implementation of NHIN must be accompanied by a significant public education program so that people understand the value of the network, its privacy and security protections, how to participate in it, and the rights and benefits afforded to them.

- The NHIN must permit patients to transmit information to their health care providers as well as receive information from them.

Governance

- Consumer and patient advocates must be represented on an equal footing in the governance and advisory structure of all regional and national NHIN authorities, including standard-setting and operational entities.

- The governance and administration of the NHIN must be public, transparent, and accountable.