CONNECTING FOR HEALTH
COMMON FRAMEWORK

Resources for Implementing Private and Secure Health Information Exchange

A Common Framework for Connecting Americans to Their Personal Health Information

Carol Diamond, MD, MPH
Managing Director
Markle Foundation

What is Connecting for Health?

- A public-private collaborative of 100+ organizations representing all the points of view in healthcare.
- A neutral forum.
- Founded & supported by the Markle Foundation
- Additional support from the Robert Wood Johnson Foundation

What is the Purpose of Connecting for Health?

To catalyze the widespread changes necessary to realize the full benefits of HIT, while protecting patient privacy and the security of personal health information.

The Connecting for Health Model

- Sharing = linking existing sources of information
- Health information can *stay where it is*—with the doctors and others who created it
- Specific information is shared *only* when and where it is needed.
- Sharing *does not* require an all new “network” or infrastructure
- Sharing *does not* require a central database or a national ID
- Sharing *does* require a Common Framework

A Common Framework Is Needed

- The Common Framework is the minimum necessary set of rules or protocols for *everyone* who shares health information to follow.
- Helps organizations overcome the barriers without “reinventing the wheel”
- Enables nationwide interoperability…avoiding isolated islands of information
- Builds *trust*

The Common Framework

- A core set of technical standards and policies that *everyone* who shares health information electronically should follow to protect the privacy and security of personal health information.
- Represents a consensus-based balance between the need to share personal health information electronically and the need to protect it from inappropriate access or use.
- A nationwide set of traffic rules that guide personal health information exchange among health care providers in order to improve consumers' access to, autonomy over, and confidentiality of this information.

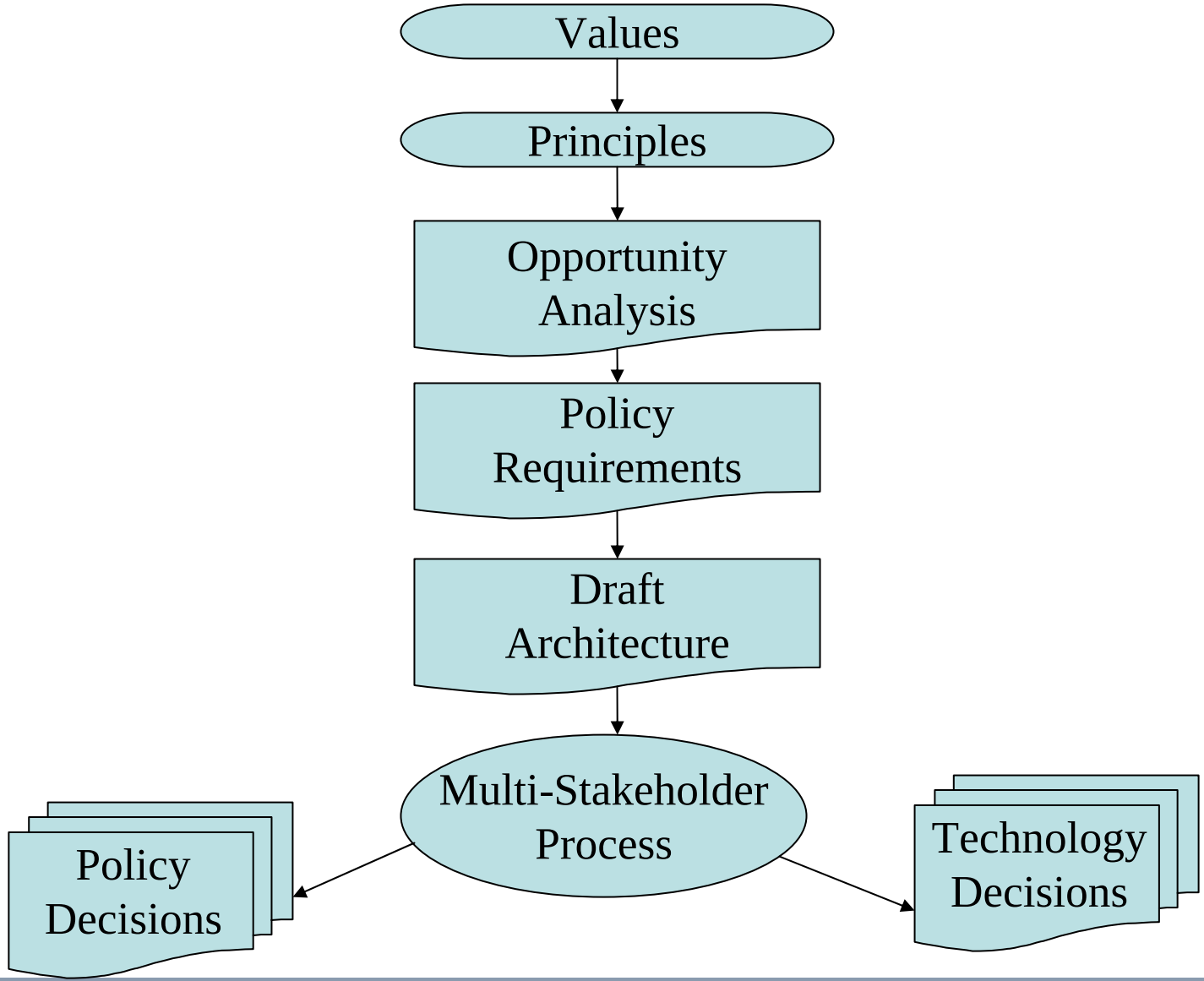
Design Principles of the Model

- Designed to safeguard privacy— we identified the values and requirements and *then* designed the technical architecture
- Patient information remains where it is now and is not kept in a central database (“decentralized”)
- Built without a national patient ID
- Leverages both “bottom-up” and “top-down” strategies
- Builds on existing systems (“incremental”) and creates early value for doctors and patients
- Consists of an interoperable, standards-based “network of networks” built on the Internet
- Data-sharing initiatives have local autonomy but follow certain ***standards and policies*** to enable interoperability (“federated”)

Getting the Technology Right is Often Easier!

To build trust, policy principles derived from shared American vales must precede, and in fact determine, the design of the network.

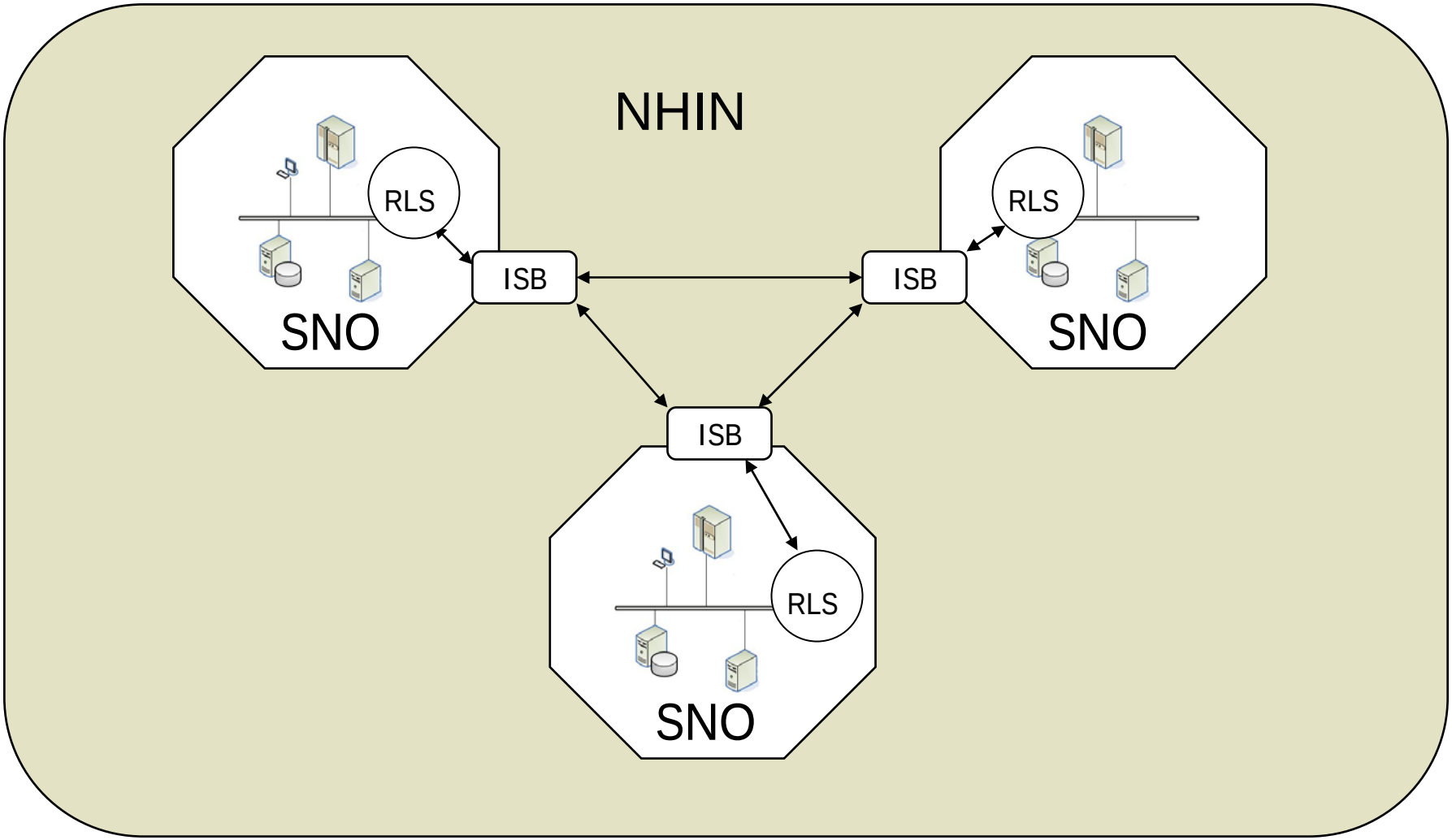
CFH's Model for Networking PHRs



Consumer- and Patient-Focused Principles for Handling Electronic Personal Health Information

- Individuals should be guaranteed access to their own health information.
- Individuals should be able to access their personally identifiable health information conveniently and affordably.
- Individuals should know how their personally identifiable health information may be used and who has access to it.
- Individuals should have control over whether and how their personally identifiable health information is shared.
- Systems for health information exchange must protect the integrity, security, and confidentiality of an individual's information.
- The governance and administration of health information exchange networks should be transparent and publicly accountable.

Common Framework Architecture for Institutional Interoperability



How Consumers Could be Networked Via the Common Framework

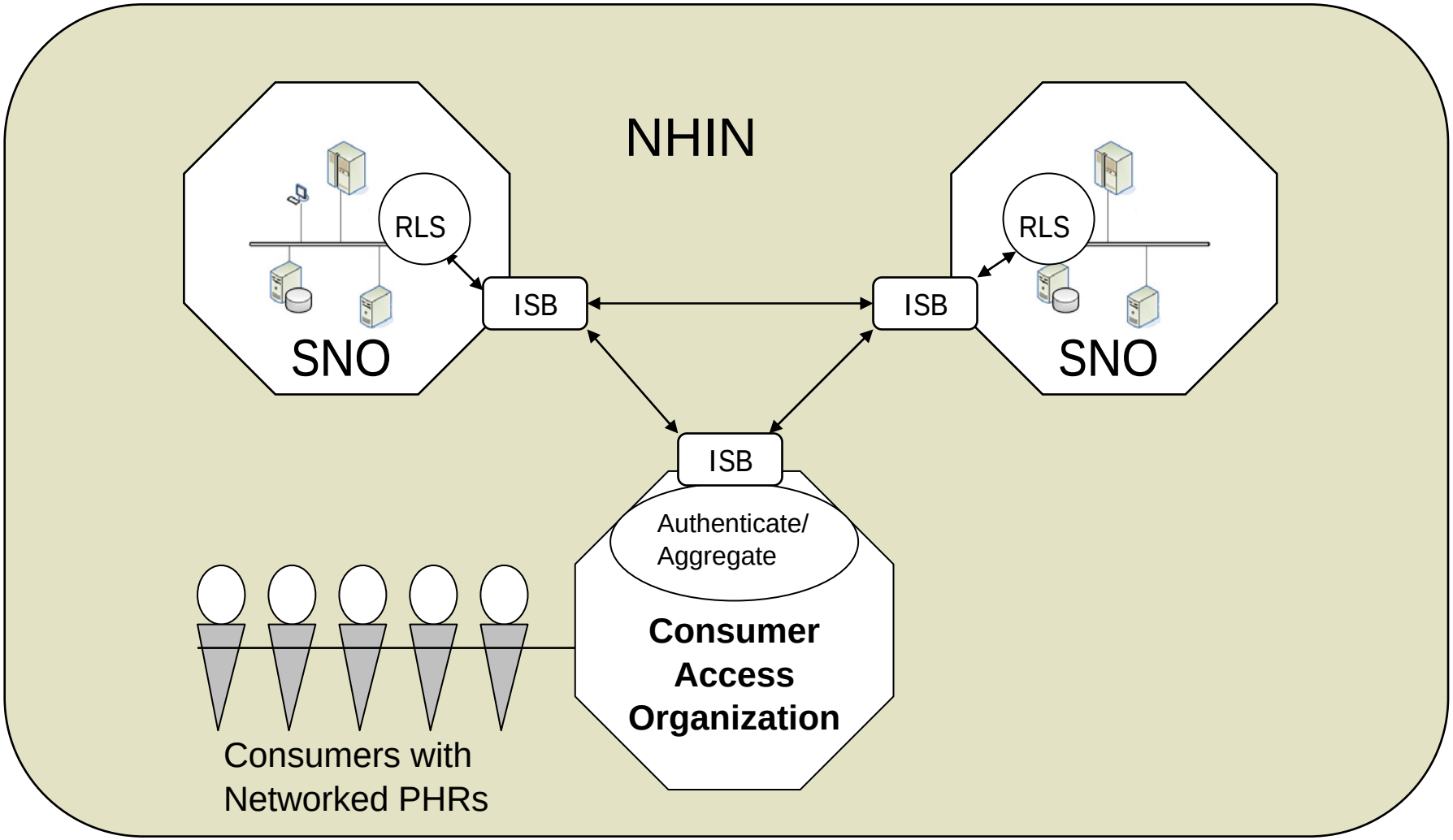
Fundamental design elements would not be changed since consumer access has always been a design principle of the Common Framework.

Individual Consumers Will Need Intermediating Bodies to Facilitate Their Access to the Network

Functions:

- aggregate consumers
- issue them identity credentials and “vouch” for them as network users
- assure that network-wide policies (e.g., privacy and information practices) are followed

Consumer Access Organizations (CAOs)



Challenges: Defining the “Rules of the Road”

1. What qualifications must a Consumer Access Organization possess?
2. What policies, contracts, and other governing mechanisms should be applied to these organizations?

CFH's Work Groups are Focusing on Two of Many Policy Issues

- **Authentication:** How does a network participant know that a consumer user is really who she says she is?
- **Consumer Access Organization policy requirements:**
  - What are the key principles and characteristics of a CAO?
  - What specific capabilities and liabilities must a CAO assume to maintain a chain of trust with other network participants?

Creating an Environment of Trust is Critical

- There must be a Common Framework of policies for information sharing among network participants to successfully develop an open market of networked PHRs.

How to Achieve a National Vision of Networked PHR's for All?

- Need consensus on the characteristics of the network and the way personal health information will be shared and managed.

Common Framework Resources

- All available free at www.connectingforhealth.org
- Policy and technical guides, model contractual language
- Registration for AHRQ/NORC Common Framework discussion forum
- Software code from regional prototype sites: Regenstrief, MAShare, OpenHRE
- Email to info@markle.org