CP1 CP2 CP3 CP4 CP5 CP6 CP7 CP8 CP9

CT1 CT2 CT3 CT4 CT5 CT6 **CT7**

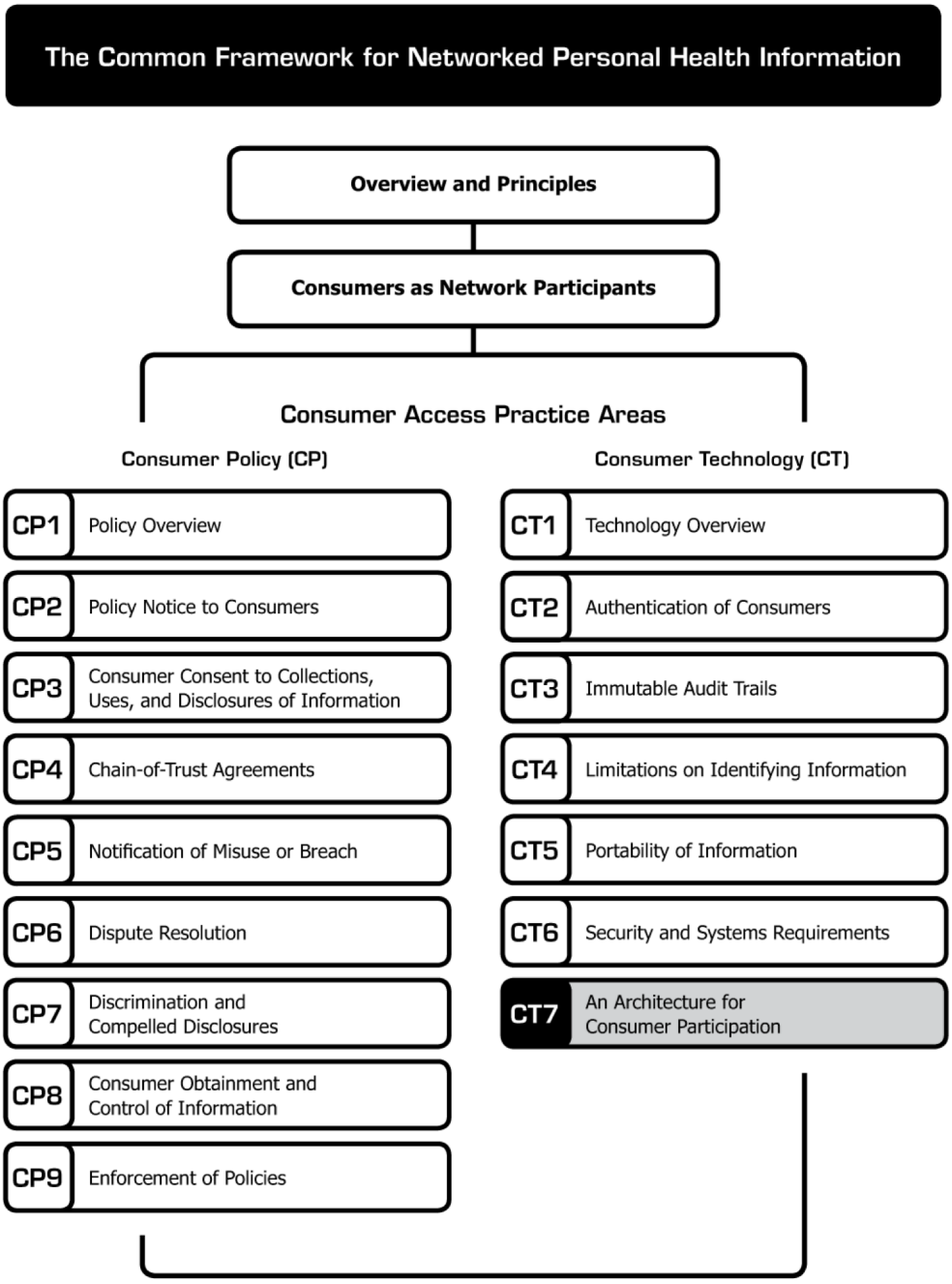
An Architecture for Consumer Participation

An Architecture for Consumer Participation

The document you are reading is part of the ***Connecting for Health*** *Common Framework for Networked Personal Health Information*, which is available in full and in its most current version at http://www.connectingforhealth.org/.

This framework proposes a set of practices that, when taken together, encourage appropriate handling of personal health information as it flows to and from personal health records (PHRs) and similar applications or supporting services.

As of June 2008, the Common Framework included the following published components:



An Architecture for Consumer Participation*

Purpose: This paper considers how consumer access to personal health information fits within the **Connecting for Health** Common Framework approach to a Nationwide Health Information Network (NHIN). To begin, there are two critical considerations:

1. In our vision, the NHIN is not a new network, but rather a way of using the existing Internet for private and secure health information exchange based on a set of common policies and practices.
2. Many different types of health information networks can be connected via the Internet, including local health information exchanges (HIEs), provider systems, data clearinghouses, and a rich variety of consumer-oriented applications.

The first set of **Connecting for Health** Common Framework resources, released in April 2006, was designed to enable interoperable exchange of patient data *among clinicians*. It is a substantial challenge to add consumers to the exchange. From the policy standpoint, it is necessary to develop an adequate set of information-sharing policies to which both consumers and institutional data custodians can agree. On the technical side, a network architecture must be consistent with fair information practices, and scalable and adaptable to the many combinations of relationships that consumers have with various health care entities. These technical and policy challenges must be addressed in tandem.

* **Connecting for Health** thanks Josh Lemieux, Markle Foundation; Clay Shirky, New York University Graduate Interactive Telecommunications Program; and David Lansky, PhD, for drafting this paper.

This practice area addresses the following **Connecting for Health** Core Principles for a Networked Environment*:

7. Security safeguards and controls

* "The Architecture for Privacy in a Networked Health Information Environment," **Connecting for Health**, June 2006. Available at: http://www.connectingforhealth.org/commonframework/docs/P1_CFH_Architecture.pdf.

Common Framework Technical Principles

The Common Framework prescribes several technical principles upon which health information exchange networks should be based. We summarize them below:

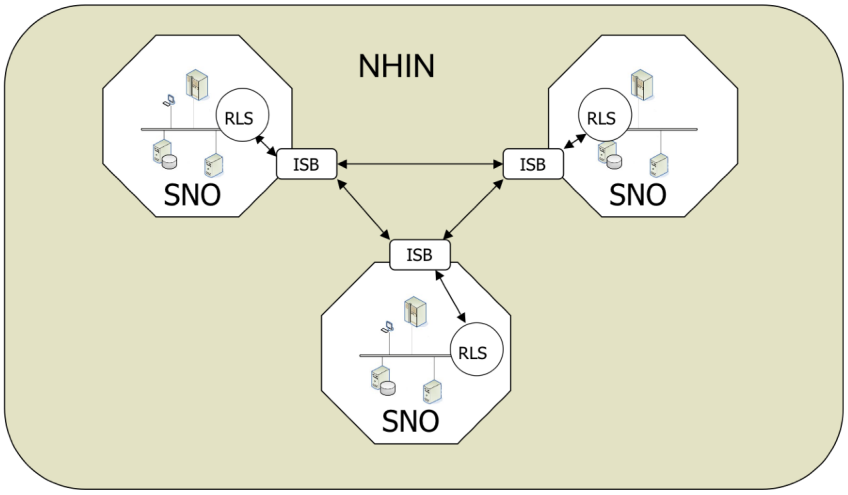
- **Make it "thin":** Data exchange networks should impose the minimal requirements for storing and transmitting health data, leaving as much processing as possible to applications at the edges of the network.
- **No requirement of a national health ID:** We argue that a national health identifier is neither likely nor necessary.
- **Avoid "rip and replace":** The health care industry has already invested heavily in technology. The network should take advantage of the technology currently in use, not require its replacement.
- **Separate applications from the network:** The roles of the network and of applications should be distinct. The purpose of the network is simply to transfer data. All other data-related functions should reside at the application level. This architecture provides for a stable infrastructure upon which application developers may build innovative functions.

- **Local control of data:** This principle holds that data not need be centralized in a new database in order for it to be shared among authorized parties, and that data may be shared directly (i.e., point to point) among authorized parties according to a consumer's needs and wishes. The primary responsibility to maintain accuracy of information should reside with the organization that captured it. However, as we discuss below, nothing in this principle should prevent a consumer from aggregating copies of her health information from multiple sources into a centralized service, if that is what the consumer wants.
- **Federation:** A federation of network members based on mutual agreements is necessary given the complexities of a decentralized network.
- **Flexibility:** The network should be designed such that it can scale and adapt over time and allow participation by a wide variety of network members.
- **Security and privacy:** Privacy protection and security should be top priorities that guide the design and development of the network.
- **Accuracy:** All reasonable efforts should be made to identify people accurately and maintain accurate records. There should be well-documented methods for identifying and correcting inaccurate information.

Connecting for Health put these principles into practice in a three-region prototype documented in previous Common Framework technical and policy papers. This paper adds to a compendium of policy resources for interoperable electronic health information exchanges. Those resources consist of:

- An overarching "architecture" for privacy based on nine interdependent principles.
- Model privacy policies and procedures.
- Notification and consent policies.
- Policies for correctly matching patients with their records.
- Policies for authentication of system users.
- Patient information access rights summary based on the Health Information Portability and Accountability Act (HIPAA).
- Policies for audit logs.
- Policies for breaches of confidential health information.[§]

The fundamental design elements of the **Connecting for Health** approach to network architecture would not be changed by granting consumers access to the network. In fact, consumer access has always been a design principle of the work. Below we review some of the key architectural concepts described more fully in prior Common Framework reports.



[§] The **Connecting for Health** Common Framework Policy and Technical Resources are available at: http://www.connectingforhealth.org/commonframework/overview.html.

- **Nationwide Health Information Network (NHIN):** As its name implies, the NHIN is an overarching network that connects exchange networks within the nation. Thus, it is envisioned as a network of networks.
- **Regional Health Information Organization (RHIO):** The current trend in health information exchange is to build provider-centric, regionalized networks. These networks are usually referred to as RHIOs. A functioning RHIO would connect multiple provider institutions in a region, such as a state or county.
- **Sub-Network Organization (SNO):** A Sub-Network Organization is a business structure comprised of entities that agree to share personal health information in accordance with a minimum set of technical and policy requirements embodied in the Common Framework. A SNO may be organized on a geographic basis (i.e., a RHIO) or in support of other business relationships that are not determined by location. For instance, the Veterans Administration (VA) has a network of hospitals and clinics that exchange health information on a nationwide level. Both RHIOs and non-regional networks like the VA would be sub-networks of the NHIN. Thus, we prefer the term "SNO" because it is a more inclusive term than RHIO.
- **Record Locator Service (RLS):** As its name implies, the RLS is a service that queries the locations of patient records within a SNO. Each SNO has its own RLS. The purpose of an RLS is best described by an example. A physician or other health care professional may wish to retrieve data on a patient from other institutions that the patient has visited. The physician would send a query to the RLS, which returns a list of record locations, but not the data itself. Thus, the RLS might inform the doctor that her patient has medical records at institutions X, Y, and Z. The contents of those records are not revealed by the RLS. Retrieval of data contained in an identified record is a separate process that occurs directly between the requesting physician and the institution that stores the record.
- **Inter-SNO Bridge (ISB):** A physician might want to search for records outside his SNO. Thus, he would send a query to the RLS of another SNO. The ISB is the conduit through which these queries and responses flow. Each SNO would have an ISB, which would be its single gateway for channeling all requests and responses from other SNOs.

In summary, the Common Framework architectural vision is a network of networks (one NHIN made up of many SNOs). Each SNO uses an RLS to locate the consumer's records and an ISB to talk to other SNOs. Institutions that want to share information across the network must be members of a SNO, comply with Common Framework policies, maintain an RLS or equivalent service, and build an ISB.

As noted in ***CT1: Technology Overview***, many important pieces of the consumer's record are already held in digital format. The custodians of this information include:

- Health insurance plans (both private and public).
- Pharmacy services and clearinghouses.
- Nationwide laboratory services.
- Self-insured employers' data warehouse services.
- Large, integrated delivery networks.
- And, to a lesser extent, some small hospitals and smaller-practice EHRs.

How Consumers Could Be Networked Via the Common Framework

Most currently available PHRs either rely on existing data silos (i.e., patient portals offering access to non-interoperable health records) or create new silos (i.e., consumer-populated, non-interoperable records). Potential large-scale benefits of PHRs are unlikely to materialize if these applications remain dependent on limited data sources.[1] For PHRs to become more universally useful to consumers, they must provide a convenient and secure means of connecting to personal data and interactive services from multiple sources, *and* they must provide a convenient and secure means of moving the data out of the PHR as well, in whole or in part.

A number of architectural approaches could permit consumers to deliver information from disparate data sources into a PHR and vice versa. At one end of the spectrum, the PHR could rely entirely on a **centralized database of personal health information**. A master database at the center of the network would aggregate data from other health information systems before the information becomes accessible in the PHR. Theoretically, the consumer could then have access via one interface to the central data repository, with potentially greater efficiencies than could be provided by queries across a distributed network. The primary problems with this centralized approach are:

1. **Data management:** Copying all personal health data to a single database, and keeping it all up to date, is impractical at population scale given the vast amounts of data that exist across systems.
2. **Data quality:** Sending all data to a central database may magnify data quality problems (although such an effort may also reveal data problems). The centralized repository model would make error checking and data reconciliation difficult compared to a model that keeps personal health information close to the entity that creates it and knows the patient. Organizations closest to the consumer are in the best position to validate, adjudicate, or update the consumer's data.
3. **Business case:** It is implausible that any one entity can emerge to garner the trust of all health care systems and all consumers in the fragmented U.S. health care environment. A single, central database would raise questions central to trust such as who controls the data, who governs the process, what secondary uses and resale of data will be allowed, etc. A single source of control for the database would risk the shortcomings of monopolies in general: low innovation, poor customer service, and higher prices. It also limits the power of the network to grow organically and incrementally.
4. **Security and privacy:** While breaches are a concern for all information holders, a centralized model poses significant risk to privacy since a single security breach could lead to a catastrophic data leak.

Centralized systems can provide valuable efficiencies and controls, and may be very appropriate at various network nodes, which should have flexibility with regard to data-storage solutions for the information that they each hold. If centralization is the only model by which health information can be shared across disparate entities, however, there is a high risk that many entities will not participate.

The polar opposite of the centralized architecture is an **entirely peer-to-peer network**. Under this model, a consumer would have to create and manage separate data streams between her PHR and each system that holds her data. The primary problems with the completely decentralized approach are in many ways the mirror image of the problems of absolute centralization:

[1] National Committee on Vital and Health Statistics [homepage on the Internet]. Washington: Department of Health and Human Services; [updated 2005 September 9; cited 2006 May 8]. September 9, 2005 Letter to Secretary Leavitt on Personal Health Record (PHR) Systems; [about 16 screens]. Available at: http://www.ncvhs.hhs.gov/050909lt.htm.

1. **Data management:** If each consumer is expected to aggregate her data, she will become both her own registrar and her own system administrator. This burden will be too much for the majority of consumers.
2. **Data quality:** Clinical data comes in both highly structured and very unstructured forms. The consumer would be responsible for managing these disparate forms of data — again, a task too challenging for most consumers.
3. **Business case:** Each person would pay for (or choose a sponsorship model for) a PHR, but the system would be highly fragmented and create few economies of scale.
4. **Security and privacy:** The security risk would be multiplied across many servers with varying levels of technical support and policy compliance. However, the breach of any given source of data would be more limited, reducing the potential for catastrophic data disclosures.

The pure point-to-point approach would place too much burden on the consumer to establish electronic transaction relationships with all of her health care services. It also would be cumbersome and pose high risks for each of the consumer's data sources, given the current lack of standards for clinical information or of a trusted mechanism to authenticate each consumer. Further, providers would be less likely to access and use the consumer's data if they were confronted with a hodgepodge of information aggregated from a series of unstructured point-to-point transactions.

How Could Consumers Aggregate Their Data?

Creation of centralized data repositories should not be an architectural requirement for data sharing, however, data aggregation at the level of the consumer could be very beneficial. How, then, can the individual aggregate her health data without relying upon a single repository at the center of the network or learning to manage a completely peer-to-peer model?

Any practical strategy for networking PHRs must avoid the negative consequences of these two extremes while satisfying the consumer's need to access and control her information.

The Common Framework vision of a federated, decentralized network of SNOs was created to meet this core requirement. Under the Common Framework, authorized clinicians are able to query the network (e.g., request an index of the locations of a patient's records) on the basis of their organization's membership in a SNO. To establish a chain of trust, the participating SNOs must have common understandings and expectations, such as how to authenticate and authorize clinicians to use the network and how to log their actions.

Consumers also need a chain of trust to interconnect across networks. Yet they represent a greater challenge than clinicians for authentication, authorization, liability, and security. There is no commonly accepted set of practices today to provide credentials to consumers for health information exchange across different systems and data repositories. It is reasonable to expect that consumer applications could become more easily "networked" if such a set of common practices existed — that is, if some type of enforceable arrangement required all participants to operate under a common set of policies and agreements to mitigate risks such as misidentification or identity theft.

In the **Connecting for Health** model, a network of interconnected SNOs is viewed as the most flexible and practical means to untether applications from data silos, as well as to enforce a common set of rules among participants. To integrate PHRs into the NHIN, we assume that the same model for connecting users — a chain of trust, brokered by an ISB that can talk to other entities in the system — must be available to patients and consumers. This paper considers the functions and requirements of an entity that provides consumers with access to the nationwide network of SNOs.

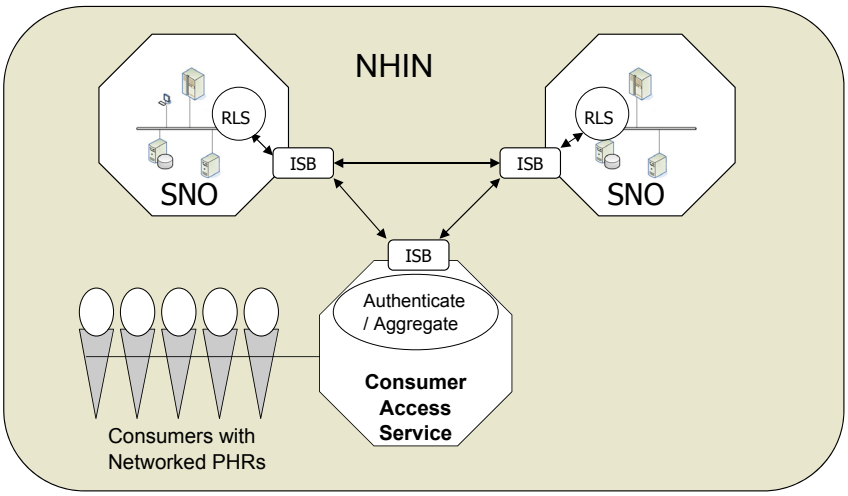
Consumer Access Services Could Act as Intermediaries

We start with three assumptions about how consumers could gain access to their data in the future. The first is that there will be services acting on the consumers' behalf as aggregators of personal health information. Other kinds of networked services with many sources of data, from e-mail to online bill paying to airline booking sites, aggregate data on behalf of the user. It may become technically possible for the consumer to access her health data (via a personal computer) directly from the hospitals, labs, and other organizations that hold it. However, even in such a scenario, many services will arise to hold and manage the data on the consumer's behalf. Issues of backup, remote access, and economies of scale are in fact already driving the creation of these sorts of services. (Some models may offer storage services of all of the consumer's data; others may emerge simply as gateways for access without actually storing the data. Ideally, consumers would choose which aggregation model best serves them.)

The second assumption is that there will be services that issue identity and authentication credentials to the consumer and pass those credentials or proof of authentication to other organizations in the NHIN, on the consumer's behalf. Today, we have no generally accepted methods or policies for initially proving the identity of each individual for the issuance of online credentials based on that identification, nor for the initial and repeated authentication of that individual's identity in an online environment. In a nationwide health information network, those who hold personal health data will need to be confident that the person to whom they transmit data is indeed who she claims to be. Common, reliable policies for initial proofing and repeated verification of identity will be essential functions of these intermediary services. (Although a complex set of issues surround identity, authentication, and authorization, we will group all of these issues under the label "authentication" for the rest of this document.)

Given the high cost of the initial consumer identification and the low cost of the subsequent authentications, economies of scale will drive the creation and growth of these functions. These intermediary services would be contractually obligated to comply with the rules governing participation in the network. Likewise, they would be expected to enforce those rules in the event of any violation by one of their authorized users (and to successfully exclude unauthorized users). By the same logic, the entities that issue identity credentials to individual consumers must have the organizational standing to enforce nationwide policies within their network. *(See **CT2: Authentication of Consumers**.)*

Third, we assume that the aggregation and authentication functions will be combined. While aggregation and authentication could be offered separately, the economic logic driving the creation of the services will also drive their combination. As a result, competing services would act as proxies for many consumers, potentially millions at a time, holding both their authentication tokens and their data. These authentication/aggregation service providers would not necessarily be covered entities under HIPAA. We call them "**Consumer Access Services.**" We will also assume that the interaction between Consumer Access Services and other entities in the NHIN will use the service-oriented architecture of the Common Framework, including both SOAP messages and message brokering by Inter-SNO Bridges.



Following the diagram above, such a combined authenticating and aggregating service would perform key NHIN functions including, at a minimum, authenticating individual users, providing an ISB interface to bridge between those users and the rest of the NHIN, and aggregating information into PHRs on those users' behalf.

A number of entities may be interested in offering these combined services to enable consumer access to the NHIN, including the following examples:

- **Provider organizations** could strengthen their role as primary care providers and care coordinators by accessing all of a patient's data when authorized and playing the role of interpreter and coach.
- **Health insurance plans and government programs** (e.g., Medicare, Medicaid, VA) could apply their data analytic- and decision support-capabilities to the clinically rich patient data available across the network and compete on their ability to deploy beneficial interventions based on that analytic intelligence.
- **Pharmacy services** (i.e., pharmacy benefit managers, retail pharmacies, clearinghouses) could offer new services to attract consumers.
- **Application vendors** could benefit from a more efficient marketing and distribution environment by offering their products to a range of Consumer Access Service suppliers with large populations of consumers.
- **Affinity and patient advocacy groups** could create their own intermediary services to help members select and use appropriate products, while using aggregate data as a platform for improving health and advocating for shared concerns.
- **Employers** could steer employees toward Consumer Access Services that allow secure access to personal health information and other benefits.
- **Web portals and other non-traditional health care players** could enter the health care space, both leveraging their brand credibility and gaining appropriate access to data that the consumer wants them to have without negotiating separate access agreements with each trading partner.
- **Regional Health Information Organizations (RHIOs)** could offer services to connect consumers.

Connecting for Health wishes to enable consumers to aggregate and manage their health care data while protecting them against the misuse or loss of personal data.

Public policy must make it possible for each person to access personal health information regardless of where it was originally acquired and where it is now maintained. In solving a problem like authentication, the NHIN needs to make sure that every American has an opportunity to gain the necessary credentials and take advantage of the information channels that exist, without being subservient to any particular gatekeeper.

Acknowledgements

This framework is a collaborative work of the **Connecting for Health** Work Group on Consumer Access Policies for Networked Personal Health Information — a public-private collaboration operated and financed by the Markle Foundation. **Connecting for Health** thanks Work Group Chair David Lansky, PhD, Pacific Business Group on Health, for leading the consensus development process for this framework, and Josh Lemieux, Markle Foundation, for drafting and editing the documents. We thank Carol Diamond, MD, MPH, managing director at the Markle Foundation, for developing the conceptual structure for this approach to networked personal health information. We particularly thank the members of the Work Group, whose affiliations are listed below for identification purposes only, for reviewing several drafts of these documents and improving them invaluably each time.

Jim Dempsey, JD, Center for Democracy and Technology; Janlori Goldman, JD, Health Privacy Project and Columbia University School of Public Health; Joy Pritts, JD, Center on Medical Record Rights and Privacy, Health Policy Institute, Georgetown University; and Marcy Wilder, JD, Hogan & Hartson LLP, made important contributions to the policy framework. Matt Kavanagh, independent contractor, and Clay Shirky, New York University Graduate Interactive Telecommunications Program, made important contributions to the technology framework. Stefaan Verhulst of Markle Foundation provided excellent research, and Jennifer De Pasquale and Michelle Maran of Markle contributed to this framework's final proofreading and production, respectively.

Connecting for Health Work Group on Consumer Access Policies for Networked Personal Health Information

Lead

David Lansky, PhD, Pacific Business Group on Health (Chair)

Staff

Matt Kavanagh, Independent Contractor
Josh Lemieux, Markle Foundation

Members

Wendy Angst, MHA, CapMed, A Division of Bio-Imaging Technologies, Inc.

Annette Bar-Cohen, MPH, National Breast Cancer Coalition

Jeremy Coote, InterComponentWare, Inc.

Maureen Costello, Ingenix

Diane Davies, MD, University of Minnesota

James Dempsey, JD, Center for Democracy and Technology

Stephen Downs, SM, Robert Wood Johnson Foundation

Joyce Dubow, AARP

Thomas Eberle, MD, Intel Corporation and Dossia

Lisa Fenichel, Health Care For All

Stefanie Fenton, Intuit, Inc.

Steven Findlay, Consumers Union

Mark Frisse, MD, MBA, MSc, Vanderbilt Center for Better Health

Gilles Frydman, Association of Cancer Online Resources (ACOR.org)

Melissa Goldstein, JD, School of Public Health and Health Services Department of Health Sciences, The George Washington University Medical Center

Philip T. Hagen, MD, Mayo Clinic Health Solutions

Robert Heyl, Aetna, Inc.

David Kibbe, MD, MBA, American Academy of Family Physicians

Jerry Lin, Google Health

Kathleen Mahan, MBA, SureScripts

Ken Majkowski, PharmD, RxHub, LLC

Philip Marshall MD, MPH, WebMD Health

Deven McGraw, Center for Democracy and Technology

Kim Nazi*, FACHE, U.S. Department of Veterans Affairs

Lee Partridge, National Partnership for Women and Families

George Peredy, MD, Kaiser Permanente HealthConnect

Joy Pritts, JD, Center on Medical Record Rights and Privacy, Health Policy Institute, Georgetown University

Scott Robertson, PharmD, Kaiser Permanente

Daniel Sands, MD, MPH, Cisco Systems, Inc.

Clay Shirky, New York University Graduate Interactive Telecommunications Program

Joel Slackman, BlueCross BlueShield Association

Anna Slomovic, PhD, Revolution Health

Cynthia Solomon, Follow Me

Ramesh Srinivasan, MedicAlert Foundation International

Michael Stokes, Microsoft Corporation

Susan Stuard, New York-Presbyterian Hospital

Paul Tang, MD, Palo Alto Medical Foundation/ Sutter Health

Jeanette Thornton, America's Health Insurance Plans

Frank Torres, JD, Microsoft Corporation

Tony Trenkle*, Centers for Medicare & Medicaid Services

Jonathan Wald, MD, Partners HealthCare System

James Walker, MD, FACP, Geisinger Health System

Marcy Wilder, JD, Hogan & Hartson LLP

Anna Wong, Medco Health Solutions, Inc.

Matthew Wynia, MD, MPH, CAPH, American Medical Association

Teresa Zayas-Caban, PhD*, Agency for Healthcare Research and Quality

**Note: State and Federal employees participate in the Personal Health Technology Council but make no endorsement.*