CP1 CP2 CP3 CP4 CP5 CP6 CP7 CP8 CP9

CT1 CT2 CT3 CT4 CT5 CT6 CT7

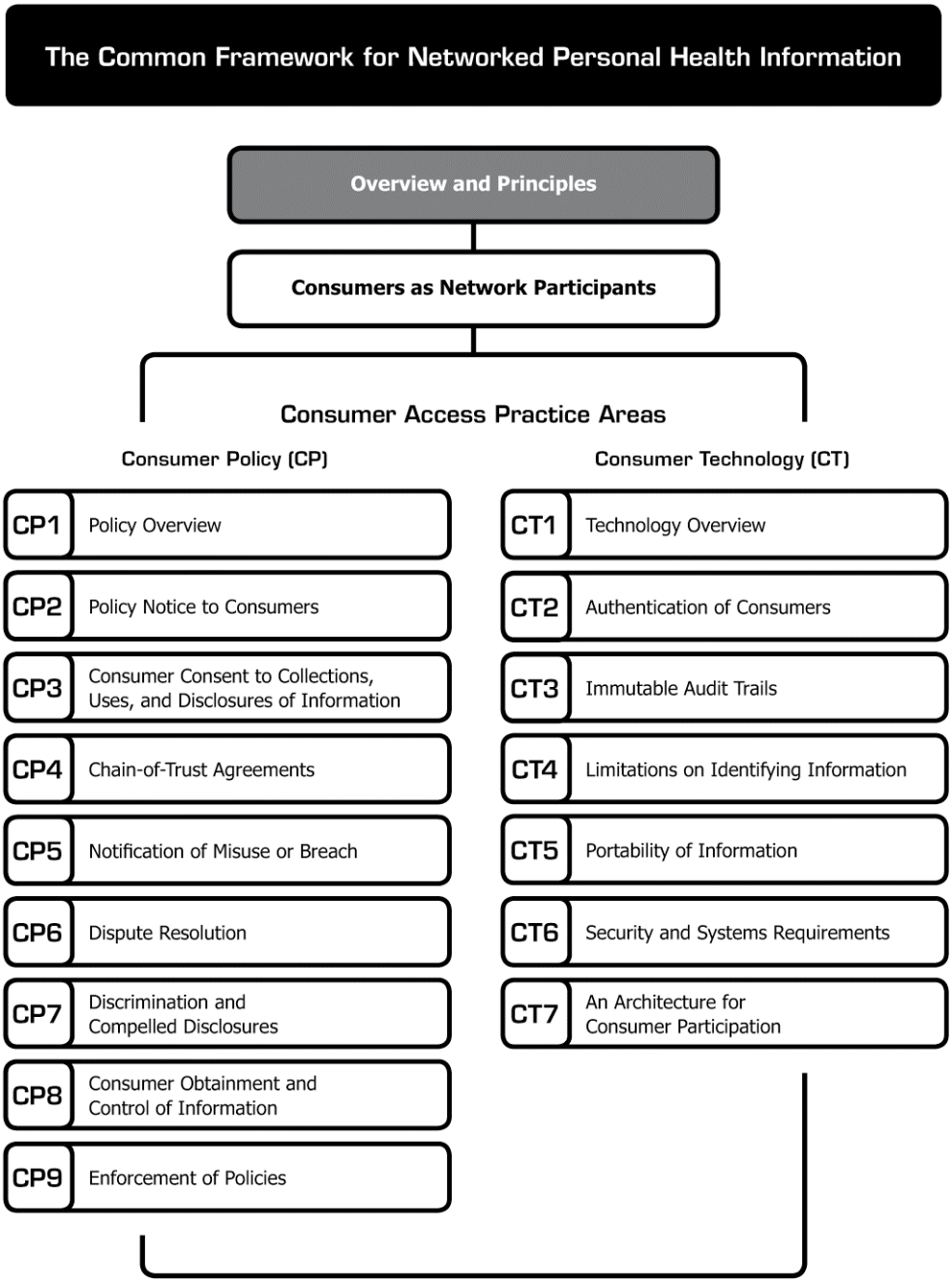
Overview and Principles

Overview and Principles

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:



Overview and Principles*

Many policy and industry leaders now agree that empowerment of consumers — enhanced by convenient access to networked health information services — will help drive necessary changes to the health care sector. The **Connecting for Health** Common Framework for Networked Personal Health Information provides a foundation for maintaining trust among all participants — business, professional, and consumer — in electronic health information networks.

The objective is to give consumers the ability to compile electronic copies of their personal health information, including their own contributions, under a set of fair practices that respect personal preferences for how information may be collected and shared. The term "networked" implies connectivity across entities. Networking health information is critical given the fragmentation of most health-related services in the United States.

Connecting for Health — a public-private collaborative group engaging more than 100 organizations representing all major components of the health sector — convened the Work Group on Consumer Access Policies[1] to identify a set of practices to support the emergence of networked personal health records (PHRs) in the public interest. PHRs include a wide variety of electronic applications designed to help consumers manage their health-related information and transactions, communicate better with clinicians, or take better care of themselves and loved ones.

The Common Framework resources are intended to foster network relationships and, ultimately, to enhance trust among the following parties:

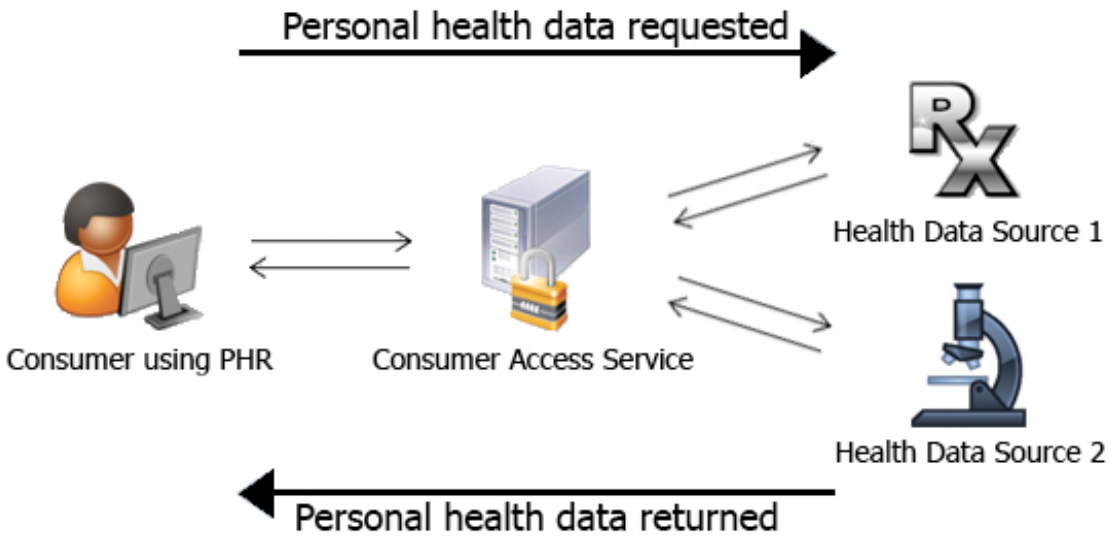
- **Consumers**, including patients, their families, and caregivers. Our vision is that individual consumers will be able to compile and share electronic copies of their personal health information captured at various points, including the home (e.g., monitoring devices, patient diaries).
- **Heath Data Sources**, meaning any institutional custodian of the individual's personal health information. This may include health care providers and clinics, hospitals and health care systems, health insurance plans, clearinghouses, pharmacies and pharmacy benefit managers, laboratory networks, disease management companies, and others that hold data related to the personal health of individuals.
- **Consumer Access Services**, an emerging set of services designed to help individuals make secure connections with Health Data Sources in an electronic environment. Consumers may be offered such services by a variety of organizations, ranging from existing health care entities (e.g., providers, payers, self-insured employers) to new entrants to the

---

* This framework is the product of the **Connecting for Health** Work Group on Consumer Access Policies for Networked Personal Health Information. *(See Work Group roster in **Acknowledgements**.)* **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 guiding the documents. We particularly thank Carol Diamond, MD, MPH, Managing Director of the Health Program at the Markle Foundation, for developing the conceptual structure for this approach to networked personal health information.

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.

[1] See **Acknowledgments** for a roster of the **Connecting for Health** Work Group on Consumer Access Policies.



health sector (e.g., technology companies, employer coalitions, affinity groups, health record banks, etc.). Such services are likely to provide functions such as authentication as well as data hosting and management.

We distinguish Consumer Access Services from PHR applications (although both could be supplied in one integrated product). Consumers ideally will have a choice of services to enable PHR applications of their choosing to exchange data with multiple Health Data Sources across a secure "network of networks."[2] The diagram above illustrates this basic distinction.

The rationale for Consumer Access Services rests primarily on two points:

1. It is not practical for most individuals to connect separately and differently to every institution that holds their health data, and
2. In an open and innovative market, individuals should choose applications that best meet their own needs, rather than be solely reliant on the applications offered by the various institutional sources of their health information or services.

The Common Framework resources are designed to guide organizations participating in what we call "consumer data streams" — the flow of personal health information into and out of consumer-accessible applications such as PHRs. (*See* ***CT1: Technology Overview*** *for a discussion of "consumer data streams" and how they contrast with "business data streams."*)

There are many emerging consumer data streams today. Hundreds of PHR applications now offer a variety of services to U.S. consumers, including products sponsored by providers, health plans, employers, technology companies, non-profits, and others. Several global brands have launched initiatives to act as Consumer Access Services. There also is a growing number of patient community sites, often described as "Health 2.0," that take innovative approaches to health problems from outside traditional health care.

Public opinion surveys commissioned by the Markle Foundation[3] and others have found that most Americans want to have electronic copies of their health records. The research indicates that Americans understand that quality of care could improve when their health information is

[2] By analogy, a cell phone is an application, and a cellular service connects the application to a network of towers that allow the phone to connect with other cell phones. Similarly, the PHR is an application, and a Consumer Access Service provides network services enabling a consumer to receive and send information through a PHR application.

[3] Lake Research Partners and American Viewpoint, commissioned by **Connecting for Health**, *Survey Finds Americans Want Electronic Personal Health Information to Improve Own Health Care*. December 2006. Available online at: http://www.markle.org/downloadable_assets/research_doc_120706.pdf.

available over the Internet to them and those who care for them. Markle also found that eight in 10 Americans are very concerned about identity theft or fraud, and the possibility of their data being used by marketers without their permission.

This Common Framework provides a voluntary approach to meet the dual challenges of making personal health information more readily available to consumers, while also protecting it from unfair or harmful practices.

Connecting for Health Core Principles

Connecting for Health has published a set of principles that provide the foundation for managing personal health information within consumer-accessible data streams. The consensus principles — based on accepted international fair information practices — are presented fully in *The Architecture for Privacy in a Networked Health Information Environment*.[4] Taken together, the nine principles form a comprehensive approach to privacy, the hallmark for which is that personal information be handled according to the individual's understanding and consent. In brief, the principles, and the corresponding papers in this Framework, are as follows:

[4] Available online at: http://www.connectingforhealth.org/commonframework/p1.html.

Connecting for Health Core Principles	Practice Areas of this Common Framework for Networked Personal Health Information
1. **Openness and transparency:** Consumers should be able to know what information has been collected about them, the purpose of its use, who can access and use it, and where it resides. They should also be informed about how they may obtain access to information collected about them and how they may control who has access to it.	***CP2:*** *Policy Notice to Consumers*
2. **Purpose specification:** The purposes for which personal data are collected should be specified at the time of collection, and the subsequent use should be limited to those purposes, or others that are specified on each occasion of change of purpose.	***CP2:*** *Policy Notice to Consumers* ***CP3:*** *Consumer Consent to Collections, Uses, and Disclosures of Information* ***CT4:*** *Limitations on Identifying Information*
3. **Collection limitation and data minimization:** Personal health information should only be collected for specified purposes and should be obtained by lawful and fair means. The collection and storage of personal health data should be limited to that information necessary to carry out the specified purpose. Where possible, consumers should have the knowledge of or provide consent for collection of their personal health information.	***CP2:*** *Policy Notice to Consumers* ***CP3:*** *Consumer Consent to Collections, Uses, and Disclosures of Information* ***CT4:*** *Limitations on Identifying Information*
4. **Use limitation:** Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified.	***CP2:*** *Policy Notice to Consumers* ***CP3:*** *Consumer Consent to Collections, Uses, and Disclosures of Information* ***CT3:*** *Immutable Audit Trails* ***CT4:*** *Limitations on Identifying Information*
5. **Individual participation and control:** Consumers should be able to control access to their personal information. They should know who is storing what information on them, and how that information is being used. They should also be able to review the way their information is being used or stored.	***CP3****: Consumer Consent to Collections, Uses, and Disclosures of Information* ***CP5:*** *Notification of Misuse or Breach* ***CP8:*** *Consumer Obtainment and Control of Information* ***CT3:*** *Immutable Audit Trails* ***CT5:*** *Portability of Information*

6. **Data quality and integrity:** All personal data collected should be relevant to the purposes for which they are to be used and should be accurate, complete, and up-to-date.	***CP6:*** *Dispute Resolution* ***CP8:*** *Consumer Obtainment and Control of Information* ***CT2:*** *Authentication of Consumers* ***CT3:*** *Immutable Audit Trails*
7. **Security safeguards and controls:** Reasonable safeguards should protect personal data against such risks as loss or unauthorized access, use, destruction, modification, or disclosure.	***CP5****: Notification of Misuse or Breach* ***CT2:*** *Authentication of Consumers* ***CT4:*** *Limitations on Identifying Information* ***CT6:*** *Security and Systems Requirements* ***CT7:*** *An Architecture for Consumer Participation*
8. **Accountability and oversight:** Entities in control of personal health information must be held accountable for implementing these principles.	***CP4:*** *Chain-of-Trust Agreements* ***CP5:*** *Notification of Misuse or Breach* ***CP6:*** *Dispute Resolution* ***CP9:*** *Enforcement of Policies* ***CT3:*** *Immutable Audit Trails*
9. **Remedies:** Remedies must exist to address security breaches or privacy violations.	***CP5:*** *Notification of Misuse or Breach* ***CP6:*** *Dispute Resolution* ***CP9****: Enforcement of Policies*

The general standard is that practices must not be misleading or unfair. Misleading practices include misrepresentations or omissions that may contribute to a reasonable consumer's decision to use a service, provide personal data, or grant permissions relating to that data.[5] Unfairness may occur when consumers are injured after being forced or coerced into making decisions in the marketplace that are not their own.[6] Emerging consumer data streams must be based on trusted and transparent relationships, without behind-the-curtain uses or disclosures of personal information that would catch an average consumer unawares. It would be alarming for consumers, as well as all legitimate network participants, if consumer data streams were harnessed by "shadow" businesses that exploit indirect and involuntary relationships with consumers.

[5] See the Federal Trade Commission's *1983 Policy Statement on Deception*. Accessed online on August 28, 2007, at the following URL: http://www.ftc.gov/bcp/policystmt/ad-decept.htm.

[6] See the Federal Trade Commission's *1980 Policy Statement on Unfairness*. Accessed online on October 22, 2007, at the following URL: http://www.ftc.gov/bcp/policystmt/ad-unfair.htm.

Practice Areas for Networked Personal Health Information

We contend that a foundational set of practices, rooted in the above principles, would help sustain public confidence in consumer data streams. We sought to propose a set of practices that, when taken together, encourage appropriate handling of personal health information. The Consumer Framework for Networked Personal Health Information introduces nine policy and seven technical resources that provide a foundation for organizations doing any of the following:

1. Collecting, receiving, storing, or using personal health information as part of a consumer data stream or PHR services.
2. Transmitting or disclosing to a third party any personal health information gathered through or derived from a consumer data stream or PHR services.

At this early point in the evolution of PHRs and services to support them, we propose this as a voluntary framework. We recommend that all organizations develop clear and public policies for each of the practice areas in this framework. *All practice areas must be addressed to provide adequate protections to consumers and to encourage trust across a network*.

The framework consists of Consumer Policy (CP) and Consumer Technology (CT) papers, although there is often not a firm distinction between policy and technology. Indeed, it is a hallmark of the Common Framework approach that decisions on policy and technology are interdependent.

Consumers as Network Participants: Explains why consumer participation can be transformative in health care as it has been in other sectors; why networked PHRs are a vital tool to empowering consumers, and how policies can help guide an emerging industry.

CP1: Policy Overview: Describes the policy landscape, including how the Health Information Portability and Accountability Act (HIPAA) as well as state and contract laws apply to emerging consumer data streams. Explains unregulated and regulated areas of the current environment, and argues for a voluntary common framework of policies.

CP2: Policy Notice to Consumers: Recommends preferred practices for giving consumers access to the policies for collection, use, and disclosures of personal health information, including privacy and security practices, terms and conditions of use, and other relevant policies.

CP3: Consumer Consent to Collections, Uses, and Disclosures of Information: Describes mechanisms to capture the consumer's agreement prior to any collection, use, or disclosure of personal data; explains why notice and consent are not sufficient by themselves in providing adequate protection for consumers.

CP4: Chain-of-Trust Agreements: Describes the merits and limitations of contractual mechanisms among parties exchanging personal health information; recommends important limitations to place on unaffiliated third parties, including vendors, service providers, and others who receive personal data or de-identified data.

CP5: Notification of Misuse or Breach: Discusses what to do if something goes wrong. Recommends that consumers be individually informed if their personal information was, or is reasonably believed to have been, disclosed or acquired by an unauthorized person or party in a form that carries significant risk of compromising the security, confidentiality, or integrity of personal information.

CP6: Dispute Resolution: Recommends that consumers be provided a clear and logical pathway to resolve disputes such as over breach or misuse, data quality or matching errors, allegations of unfair or deceptive trade practices, etc.

CP7: Discrimination and Compelled Disclosures: Recommends policies to bar discrimination and "compelled disclosures" — such as when the consumer's authorization for release of data is required in order to obtain employment, benefits, or other services.

CP8: Consumer Obtainment and Control of Information: Covers several areas to facilitate the consumer's ability to electronically collect, store, and control copies of personal health information, including requesting data in an electronic format, allowing for proxy access to an account, requesting amendments, or disputing entries of data. Also covers appropriate retention of information in inactive accounts, and consumer requests to "delete" data and terminate their accounts.

CP9: Enforcement of Policies: Raises the issue of how policies and practices should be enforced on the network; describes the pros and cons of several different enforcement mechanisms, including: enforcing current laws, amending and expanding HIPAA, creating new law to govern Consumer Access Services, encouraging self-attestation with third-party validation, and encouraging consumer-based ratings.

CT1: Technology Overview: Describes the complexity of emerging digital health data streams; explains how information can be combined to build revealing profiles of individuals; depicts how health care entities and consumer technology innovators operate under different cultures that can clash without basic rules of the road.

CT2: Authentication of Consumers: Provides a framework for establishing and confirming the identity of individual consumers so that they may participate on a network.

CT3: Immutable Audit Trails: Recommends that audit trails be a basic requirement of PHRs and supporting services; explains the value of providing consumers with convenient electronic access to an audit trail as a mechanism to demonstrate compliance with use and disclosure authorization(s).

CT4: Limitations on Identifying Information: Recommends strong limitations on disclosures of identifying data to third parties. Supports disclosures only of those data that are reasonably necessary to perform the limited function(s) to which the third parties are authorized. Provides a caveat about considering data "de-identified."

CT5: Portability of Information: Highlights the importance of the consumer's ability to export and import information in industry-standard formats as they become available.

CT6: Security and Systems Requirements: Provides a brief outline on basic security protections. Recommends continuous monitoring of industry practices and threats, as well as personnel training and strict policies regarding who can access consumer data, and consequences for security violations.

CT7: An Architecture for Consumer Participation: Provides a view on how Consumer Access Services can fit within the **Connecting for Health** approach to architecture for a Nationwide Health Information Network (NHIN).

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.*