CP1 CP2 CP3 CP4 CP5 CP6 CP7 CP8 CP9

CT1 CT2 CT3 CT4 CT5 CT6 CT7

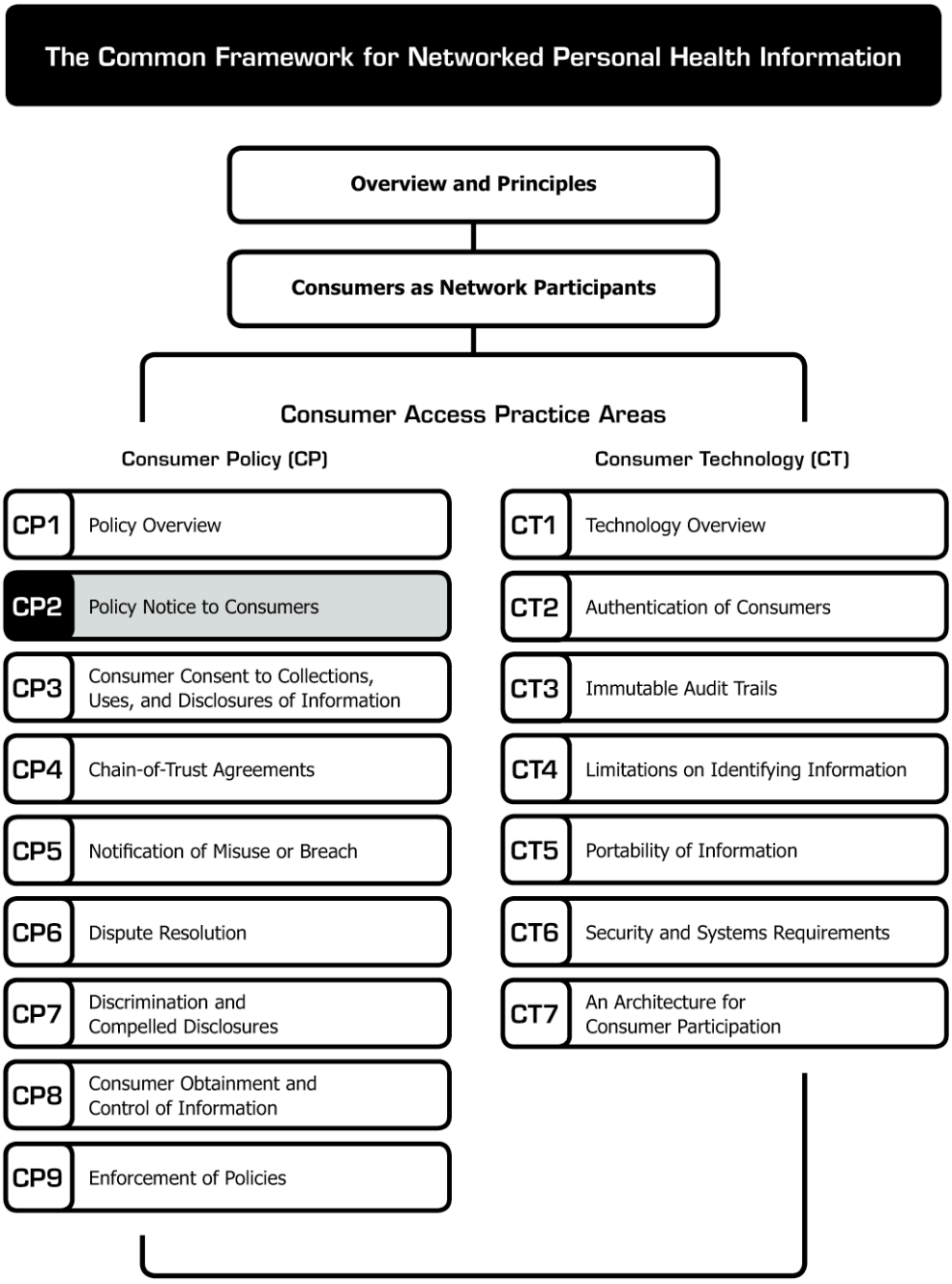
Policy Notice to Consumers

Policy Notice to Consumers

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:



Policy Notice to Consumers*

Purpose: There is general agreement that "good privacy begins with effective transparency"[1] and that consumers must be given access to information about policies for collection, use, and disclosures of personal health information, including privacy and security practices, terms and conditions of use, and other relevant policies.

It is an industry standard to post a privacy policy for online services.[2] In practice, however, there are several limitations to the effectiveness of policy notices to consumers, the most important being that consumers rarely read them (and the few who do often find them confusing). Please see **Appendix A** for a discussion of the limitations of notice and consent in today's Internet environment.

Despite the well-known limitations with current practice in implementing the openness and transparency principle, there are at least three essential and practical reasons to develop and post clear policies on privacy and terms of use:

1. Even if most consumers fail to read them, the interested consumer has the right to know what he or she is agreeing to.
2. The process of developing and promulgating public policies for health data custodianship helps organizations examine their internal policies, and correct shortcomings, if necessary.[3]
3. The posting of publicly available policies brings into play various state and federal laws and regulations that can help police the industry and provide a layer of protection to consumers. If an entity adopts a privacy policy in the absence of a legal requirement to do so, and that policy is publicly available, it is likely to be enforceable if breached through the Federal Trade Commission as "unfair or deceptive practice." Once an entity makes a policy available to its customers and patients, it makes itself accountable for adhering to those policies.

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

1. Openness and transparency

2. Purpose specification

3. Collection limitation and data minimization

4. Use limitation

* "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.

---

* **Connecting for Health** thanks Josh Lemieux, Markle Foundation, for drafting this paper.

[1] The Center for Information Policy Leadership, Hunton & Williams, LLP, *Ten Steps to Develop a Multilayered Privacy Notice*. February 14, 2006, page 1. Available at: http://www.hunton.com/files/tbl_s47Details/FileUpload265/1405/Ten_Steps_whitepaper.pdf.

[2] *TRUSTe, Your Online Privacy Policy,* White Paper. 2004, p. 5-6. Accessed online on August 16, 2007, at the following URL: http://www.truste.org/pdf/WriteAGreatPrivacyPolicy.pdf.

[3] *TRUSTe, Your Online Privacy Policy*, White Paper. 2004, page 6. Accessed online on August 16, 2007, at the following URL: http://www.truste.org/pdf/WriteAGreatPrivacyPolicy.pdf.

Consumers would be better served if there were an industry-standard online format for notice of data-handling and privacy practices. We would like to see a public-private collaborative, including industry and consumer representatives as well as web accessibility and disability experts, work on such a standardized format that would enable a general, apples-to-apples comparison across consumer-accessible health applications. Such an effort should begin with the FTC's Fair Information Practice Principles as well as the documents summarized in **Appendix A**. We offer the following as guidelines.

Recommended Practice:

PHRs and Consumer Access Services must develop privacy policies, terms and conditions of use, and other relevant policies related to the handling of health information. Such statements should be:

1. **Clearly written:** Avoid excessive jargon. To the extent possible, target 4th to 6th grade reading ability. To the extent practical, provide notice in the language(s) of the target populations.
2. **Comprehensive:** Answer the questions raised by the nine **Connecting for Health** core principles. *(See **Overview and Principles**.)* The consumer should be able to know what, how, and why information is collected, used, or shared, as well as how long it will be kept, how the consumer can exercise choices or controls over the information, and whether it can be disputed or deleted, and what procedures, if any, are in place to notify affected people in the event of breach. Policy notices should define what the Consumer Access Services consider to be personally identifying information (PII) and what information is not considered personally identifying. For the latter, notice must be clear regarding limits on the ability of Consumer Access Services or third parties to make the information "re-identifiable," such as by combining it with other databases. *(See **CT4: Limitations on Identifying Information**.)* Policy notices should provide information about whether personal information will be stored in foreign countries, or whether information collected through the Consumer Access Service will be combined with other information about the individual collected from other sources, services, or contexts. It should also spell out the organization's general policy for complying with reasonable law enforcement requests for disclosure of personal information without the consumer's consent. **Appendix B** provides a more detailed list of possible topics to consider for inclusion in policy notices to consumers.
3. **Summarized:** Present key policies and protections in summary form. Make any necessary additional detail easily accessible. For example, if additional detail is necessary, let the consumer easily click from a summarized version to a more detailed version, and vice versa. It is valuable to test different formats to reach target populations. In some cases, video or other visual or interactive techniques may be more effective than written documents.
4. **Focused on protections:** Do not merely present what the service is permitted to do. Make clear the limitations on what it will do. Refer to the nine privacy principles above.
5. **Easily accessible:** Make links to relevant policies part of the service's global navigation, footer, or other standard location for such policies (i.e., accessible from every page on the site). Post links to policies on the home page and on appropriate screens on which the consumer sets up an account or makes key decisions. Brief policy notices that relate to specific choices, and that appear at the point consumers are exercising those choices, may be more effective than long legal statements that cover many different practices and activities.

6. **Updated:** Provide adequate notice to consumers of modifications in policies. Notices of modification should specifically identify the changes made. We offer the following as preferred practices:

    a. **Versions:** Post each version of the terms of use and privacy policy with identification of version number and effective date. Specifically identify the changes made to the previous version. Retain a record of all dates and means of posting notices of changes.

    b. **Type of notice:** Each time the policies are modified, consider whether it is appropriate to obtain a new authorization from the consumer. Additional authorizations should be obtained in connection with policy modifications that materially alter the policies. Provide users with a meaningful opportunity to review material modifications regardless of whether a new authorization is required.

        - **Non-material changes:** To the extent changes do not affect material provisions of the terms of use and privacy policy, the Consumer Access Service may change such policies at any time and for whatever purpose with or without a new authorization. Notice to the user may take the form of general notice of change regarding non-material provisions of terms of use or privacy policy posted prominently on web site. In this case of non-material changes, continued use of the site under the initial authorization signifies user's consent to new terms and/or policies.
        - **Material changes:** Present consumers with appropriate notice and an option to consent to updated policies if such policies are changed in a way that materially affects their provisions or there is a material change in the business relationship (e.g., a merger, acquisition, or change of ownership of the service). Notice in such cases should be posted prominently in the end-user application (e.g., PHR). It is best practice to send an e-mail to registered users notifying them of material changes, and/or provide notice and an appropriate consent mechanism upon the user's subsequent login. Determining the appropriate consent mechanism may hinge on several factors, including the usability of the interface and the principle that consent should be "proportionate" (i.e., the more sensitive or personally exposing the changes to policy, then the more specific and discrete the mechanism to capture a consumer's consent, and vice versa). *(See **CP3: Consumer Consent to Collections, Uses, and Disclosures of Information**.)* When a Consumer Access Service seeks a new authorization, it should clearly explain the consequences of opting-in and opting-out of the new policies. For example, opting-out may require the consumer to terminate use of the Consumer Access Service. In such cases, the Consumer Access Service should provide the consumer with an easy process for both downloading and printing the user's records. *(See **CP8: Consumer Obtainment and Control of Information** and **CT5: Portability of Information**.)*

Appendix A:
Limitations of Relying on Notice and Consent

The Federal Trade Commission's Fair Information Practice Principles declare:

> The most fundamental principle is notice. Consumers should be given notice of an entity's information practices before any personal information is collected from them. Without notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information.[4]

However, current industry practices of posting policy notices provide only limited protection for even the most careful consumer. We conducted an in-depth analysis of the privacy and terms of use statements of eight different PHR products, chosen based on their relatively high levels of sophistication in data integration. The organizations studied included three large integrated delivery networks, a nationwide insurance company, a nationwide retail pharmacy company, and three independent companies offering PHRs with advertised capabilities to import professionally sourced health data for the consumer. The examination, based on publicly posted policies between June and August 2007, found challenges that will be familiar to any consumer who has signed up for software or services involving personal information over the web:

- Organizations present significantly varying degrees of purpose specification, collection, and use limitations, and offer varying granularity of individual participation and control options.
- Those differences are very difficult to compare from one site to another because the posted policies are not standardized or organized in common formats.
- Policies are typically lengthy and complex, with fine print that may be vague, highly technical, or both.
- Policies contain multiple notices about how personal data will be handled. For example, in at least one case, protections listed in an organization's privacy policy could be changed under its terms and conditions of use (both of which must be agreed to by the consumer).
- Ideally, terms and conditions would be a helpful guide to consumers, spelling out the responsibilities and protections to be undertaken by each party. However, the terms and conditions we examined were typically written from the standpoint of limiting the company's liability and obtaining broad authorization from the consumer. In fine print, for example, we found clauses that allowed disclosure of personal health information to an employer at the request of a consumer's health plan, and or a denial of accountability or redress in the event of a misuse of personal data by contracted third-party entities (i.e., a lack of "chain-of-trust" reassurances).

Other studies have had similar findings. For example, one study that looked at 60 financial privacy notices and found that most were "written at a 3rd-4th year college reading level, instead of the junior high school level that is recommended for materials written for the general public [suggesting] consumers will have a hard time understanding the notices because the writing style uses too many complicated sentences and too many uncommon words."[5] A 2002 study found that none of 80 health web sites examined had a privacy policy that would be "comprehensible to most English-speaking adults in the United States."[6] A recent study, commissioned by the American Health Information Community, examined 30 PHR privacy policies and found them to be "inconsistent" and "incomplete," noting a

[4] Federal Trade Commission, *Fair Information Practice Principles*. Accessed online on August 16, 2007, at the following URL: http://www.ftc.gov/reports/privacy3/fairinfo.shtm.

[5] Hochhauser, Ph.D, *Lost in the Fine Print: Readability of Financial Privacy Notices*. July 2001. Accessed online on August 21, 2007, at the following URL: http://www.privacyrights.org/ar/GLB-Reading.htm.

[6] J Fam Pract 2002: 51:642-645, *Reading Level of Privacy Policies on Internet Health Web Sites - Brief Report*. Accessed online on August 16, 2007, at the following URL: http://findarticles.com/p/articles/mi_m0689/is_7_51/ai_88999808.

general lack of specificity on uses and disclosures of information.[7]

The net result of such practices is an undue burden on consumers to determine what the policies say and do not say. It is not surprising that most consumers do not read online privacy or terms of use statements.[8] It's not uncommon for consumers to later be surprised by unwelcome consequences.[9] This is deeply challenging in an infant industry that requires consumer trust to survive.

It is also important to note that notice alone does not protect consumers. As evidenced by recent FTC and State Attorney General cases, a company may still be engaging in unfair practices even when providing notice to the consumer if that practice could cause significant injury and is buried deeply in a disclosure.[10]

[7] Altarum, *Review of Personal Health Record (PHR) Service Provider Market: Privacy and Security*. January 5, 2007, page 17. Accessed online on August 16, 2007, at the following URL: http://www.hhs.gov/healthit/ahic/materials/01_07/ce/PrivacyReview.pdf.

[8] The Pew Internet & American Life Project, Fox, Rainie, et al.,*The Online Health Care Revolution: How the Web Helps Americans Take Better Care of Themselves*. November 26, 2000. Accessed online on August 21, 2007, at the following URL: http://www.pewinternet.org/pdfs/PIP_Health_Report.pdf.

[9] CNET News.com, *PC Invaders*. April 12, 2002. Accessed online on August 16, 2007, at the following URL: http://news.com.com/2009-1023-885144.html.

[10] See Center for Democracy and Technology, *Spyware Enforcement*, Report. Accessed online on October 22, 2007, at the following URL: http://www.cdt.org/privacy/spyware/20060626spyware-enforcement.php citing several case studies of unfair practices buried in End User License Agreements and privacy notices, including FTC v. Odysseus Marketing, Inc, and Walter Rines, FTC Docket #042-3205; In the matter of Advertising.com, Inc. a/d/b/a Teknosurf.com, and John Ferber, FTC Docket #042-3196; and State of New York v. Direct Revenue, LLC, and Joshua Abram, Alan Murray, Daniel Kaufman, Rodney Hook.

Appendix B:
A Survey of Recommended Areas for Policy Notice to Consumer

The Federal Trade Commission's Fair Information Practice Principles are an essential starting point for online policy notice statements for consumers. The FTC's notice principle reads:

> While the scope and content of notice will depend on the entity's substantive information practices, notice of some or all of the following have been recognized as essential to ensuring that consumers are properly informed before divulging personal information:
>
> - identification of the entity collecting the data;
> - identification of the uses to which the data will be put;
> - identification of any potential recipients of the data;
> - the nature of the data collected and the means by which it is collected if not obvious (passively, by means of electronic monitoring, or actively, by asking the consumer to provide the information);
> - whether the provision of the requested data is voluntary or required, and the consequences of a refusal to provide the requested information; and
> - the steps taken by the data collector to ensure the confidentiality, integrity, and quality of the data.
>
> Some information practice codes state that the notice should also identify any available consumer rights, including: any choice respecting the use of the data; whether the consumer has been given a right of access to the data; the ability of the consumer to contest inaccuracies; the availability of redress for violations of the practice code; and how such rights can be exercised.
>
> In the Internet context, notice can be accomplished easily by the posting of an information practice disclosure describing an entity's information practices on a company's site on the Web. To be effective, such a disclosure should be clear and conspicuous, posted in a prominent location, and readily accessible from both the site's home page and any web page where information is collected from the consumer. It should also be unavoidable and understandable so that it gives consumers meaningful and effective notice of what will happen to the personal information they are asked to divulge.[11]

The following table examined documents from six organizations that have studied items that should be disclosed in a notice statement to consumers. An "X" indicates that the organization has recommended that the item be part of the notice to consumers. This table is for reference only; it does not constitute a recommendation for an industry standard notification form:

[11] Federal Trade Commission, *Fair Information Practice Principles*. Accessed online on August 16, 2007, at the following URL: http://www.ftc.gov/reports/privacy3/fairinfo.shtm.

Privacy Policy Element	ASTM	TRUSTe	URAC	OECD	Nym	H&W
TRANSPARENCY						
What organization is responsible for the information that the consumer provides?			X		X	
Does this privacy policy apply to personal information collected by phone, mail, fax, in-person encounter, or just online through the web site?					X	
What is considered personal information?					X	
Does the organization collect personally identifiable information?				X		
What personally identifiable information is collected?		X	X	X	X	X
How is personally identifiable information collected?				X	X	X
Why is this information collected?						
Are individuals aware that their personal data are being collected?				X		
Who in the organization is responsible for deciding what personal data are collected and how?				X		
Who controls personal data once they are collected?				X		
What choices are available to users regarding collection, use, and distribution of the information?	X	X			X	X
Does the organization have standards, guidelines, and regulations which apply to your collection and use of personal data?				X		
Does the organization allow visitors access to the personal data it has about them?				X		
Does the consumer have opportunities to access and make corrections related to the information, either because of requirements in law or policy in the organization?	X		X		X	X
Are there any limitations on amendment, deletion, or removal of information?			X			
Does the organization use passive tracking mechanisms and if so, why?			X			
What is the organization's business model?	X					

Privacy Policy Element	ASTM	TRUSTe	URAC	OECD	Nym	H&W
APPROPRIATE USE						
Are personal data disclosed to third parties, and if so, why?			X	X	X	X
How and where are data disclosed to third parties stored?				X		X
What personally identifiable information do third parties collect through the web site?		X				
What organization(s) collects the information?		X				
How does the organization use the information?	X	X	X	X	X	X
With whom may the organization share user information?	X	X				
How long is the information kept?	X		X			X
How is the information destroyed?	X					X
What is the policy concerning use of the PHR by individuals other than the consumer (i.e., proxies, providers)?	X					
Who can alter data in the PHR?	X					
What happens to the data in the event of the supplier's merger, acquisition, or dissolution?	X					
What is the policy for transferring the consumer's information to another site?	X					
To what extent is the consumer's information used for data-mining?	X					
Are de-identified data shared with third parties, and if so, what choices does the consumer have regarding these practices?						
How are requests for data from law enforcement and public health agencies handled?						
DATA QUALITY AND ACCURACY						
What are the quality assurance policies concerning the data?	X					
SECURITY AND ACCOUNTABILITY						
What are the measures the organization takes to protect the information under its control?	X	X				
What happens if a visitor has a query about their personal data? What if they are not satisfied with how the organization deals with their query?				X		
What internal and external audit practices does the organization follow?	X					
Can the consumer access audit data?						
ENFORCEMENT						
What mechanisms are in place to ensure that the privacy policy is enforced?						
What mechanisms are in place to provide remedies when there are security breaches or other violations of privacy?						

Sources:

TRUSTe: Your Online Privacy Policy, Whitepaper. 2004. Page 14. Available at: http://www.truste.org/pdf/WriteAGreatPrivacyPolicy.pdf.

OECD: Available at: http://www.oecd.org/document/1/0,2340,en_2649_34255_28863233_1_1_1_1,00.html.

URAC: *Health Web Site Accreditation Standards, 2.0*. Available at: http://accreditnet.urac.org/public/ProgramGuideLight.aspx?l=1&pg=131 Username: ProgramGuide; Password: URACPG16.

Nymity: *Nymity's Short Notice Guide*. Available at: http://www.nymity.com/about_us/documents/NymitysShortNoticeGuide.pdf.

Hunton & Williams,*Ten Steps to Develop a Multilayered Privacy Notice*. Available at: http://www.hunton.com/files/tbl_s47Details/FileUpload265/1405/Ten_Steps_whitepaper.pdf.

ASTM,*Standard Specification for Relationship Between a Person (Consumer) and a Supplier of an Electronic Personal (Consumer) Health Record.* Available at: http://www.astm.org/cgi-bin/SoftCart.exe/DATABASE.CART/REDLINE_PAGES/E2211.htm?E+mystore.

Another useful resource is the work of the W3 Platform for Privacy Preferences (P3P) Project. Although its work has been suspended, P3P made an important contribution toward creating a machine-readable standard for expressing privacy preferences. See http://www.w3.org/P3P/.

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.*