



CP1

CP2

CP3

CP4

CP5

CP6

CP7

CP8

CP9

CT1

CT2

CT3

CT4

CT5

CT6

CT7

## Portability of Information

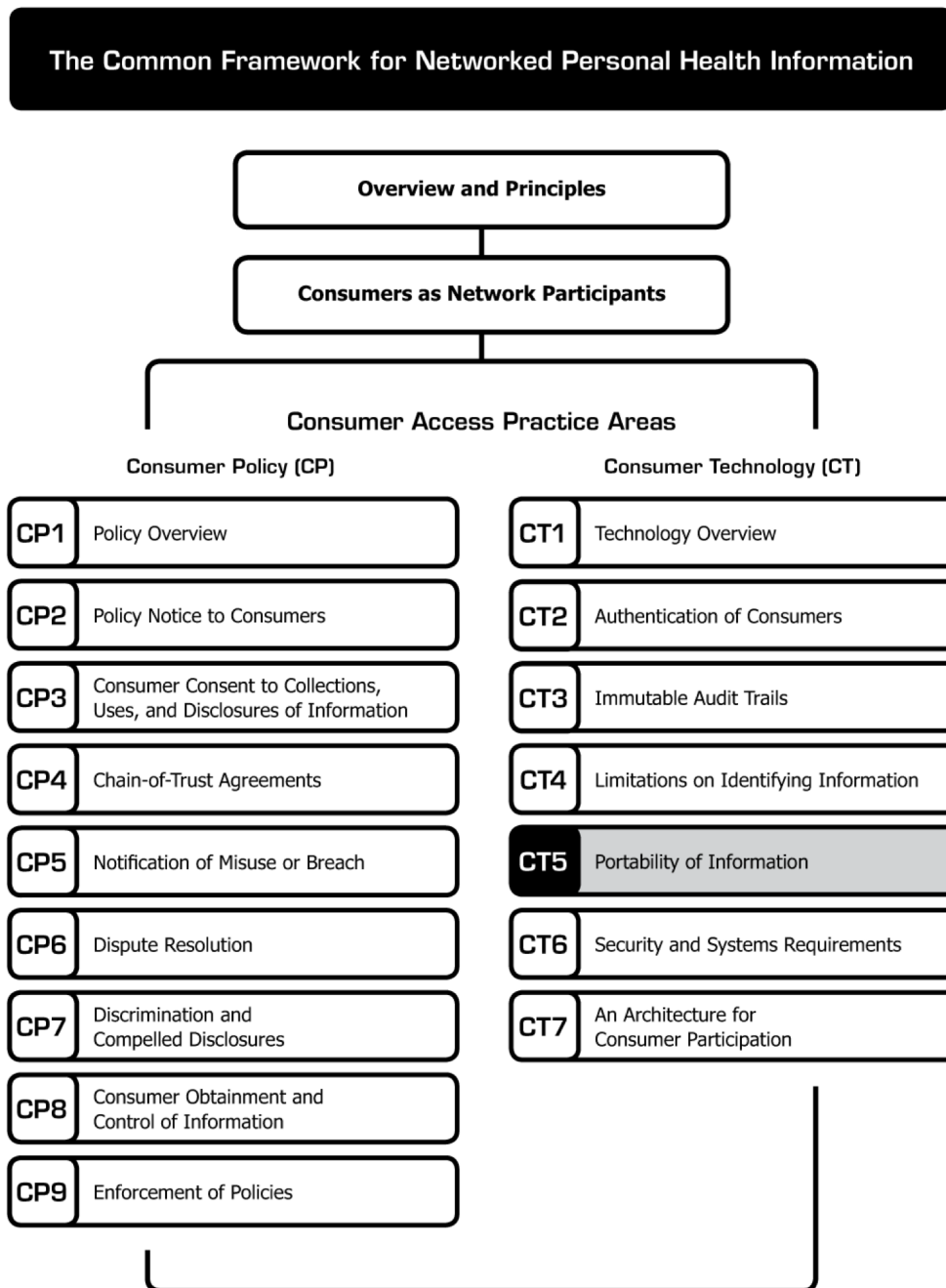
# Portability of Information

---

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:



## Portability of Information\*

---

**Purpose:** Over time, individuals move, change jobs, change providers, develop health conditions, require new services, etc. We envision a competitive market of Consumer Access Services and networked PHRs that meets the needs of many different populations at various stages of their lives. For the overall health of the emerging industry, consumers should be able to make their personally identifiable information available to any and all applications to best meet their needs.

We recommend that the industry work on standardized permissions and formats for the exporting of data from one Consumer Access Service to another upon consumer request.

### Export of Data to the Consumer

Consumer Access Services should provide mechanisms for the consumer to export information from her account in standard formats. The ideal state is that consumers would have a menu of output formats that are both human-usable and machine-readable. As health data subsets become standardized in the EHR and PHR industries, Consumer Access Services should support such standards. Ideally, Consumer Access Services would provide a mechanism for the consumer to export all data in the account in a human-intelligible format into standard software such as a spreadsheet or text file. Print capability is a reasonable minimum requirement. Once the consumer assumes full control of the copies of data (e.g., stores them on his computer hard drive), it is the consumer's sole responsibility to protect them.

---

\* **Connecting for Health** thanks Matt Kavanagh, independent contractor, and Josh Lemieux, Markle Foundation, for drafting this paper.

©2008, Markle Foundation  
This work was originally published as part of a compendium called *The **Connecting for Health** Common Framework for Networked Personal Health Information* and is made available subject to the terms of a license (License) which may be viewed in its entirety at: <http://www.connectingforhealth.org/license.html>. You may make copies of this work; however, by copying or exercising any other rights to the work, you accept and agree to be bound by the terms of the License. All copies of this work must reproduce this copyright information and notice.

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

### 5. Individual participation and control

\* "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](http://www.connectingforhealth.org/commonframework/docs/P1_CFH_Architecture.pdf).

#### *Recommended Practice:*

Consumer Access Services should provide an easy-to-use mechanism for consumers to export information in their accounts for personal use. Such mechanisms should:

- Provide information in human-readable form.
- Include audit trail information for data entries (time-, date-, and source-stamping of each diagnosis, for example). (See **CT3: Immutable Audit Trails.**)
- Include a printer-friendly format.
- Conform to industry standards for health data subsets as they become available and broadly implemented.
- Enable data to be exported into industry standard software, such as spreadsheets, PDFs, or text files.

### Export and Import of Data Among Consumer Access Services and PHRs

The ideal future state is for consumers, according to their changing needs and wishes, to be able to transfer their information from PHR service or application to another PHR service or application. Such electronic interoperability is not a market reality today. However, Consumer Access Services should support interoperable data exchange protocols and data standards as they become available and market-tested.

*Recommended Practice:*

Consumer Access Services should support industry-standard data sets for exchanging patient health information as they become available and broadly implemented. Consumer Access Services should collaborate to create a standard messaging envelope to export and import information upon the consumer's authorization.

In the absence of full data exchange interoperability, Consumer Access Services may provide consumers with storage options for documents gathered from past Consumer Access Services or other Health Data Sources. For example, a consumer could export information from one Consumer Access Service into a standard software format such as PDF and store it on her desktop, then upload those PDF documents into a secure account at a new Consumer Access Service.

(For related recommendations, **see CP8: Consumer Obtainment and Control of Information** Area 5: Expunging of Information and Area 6: Termination of Account.

See also **CT3: Immutable Audit Trails** for recommendations on tracking export and import of data.)

## 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 invaluablely 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.*