



CP1

CP2

CP3

CP4

CP5

CP6

CP7

CP8

CP9

CT1

CT2

CT3

CT4

CT5

CT6

CT7

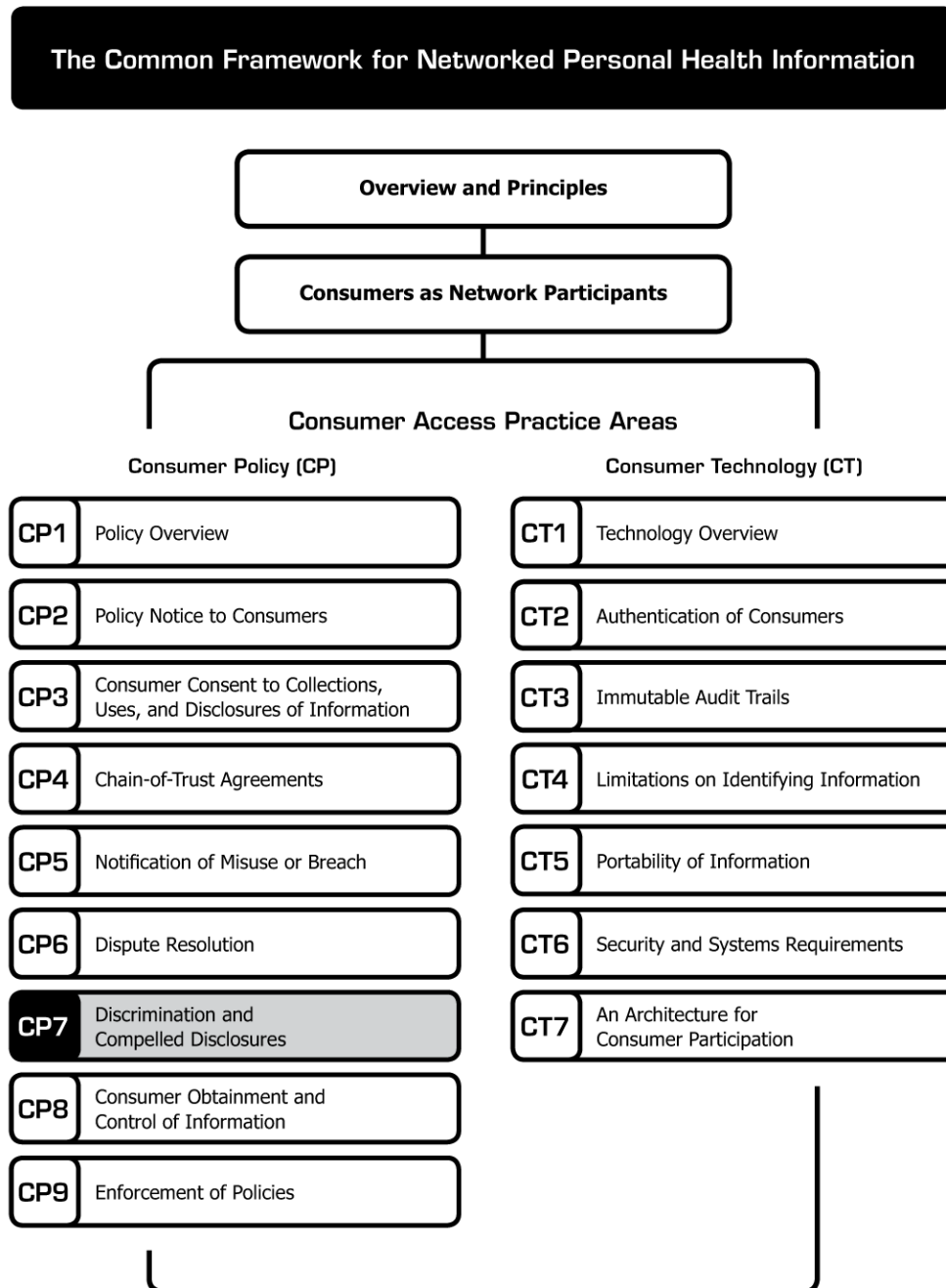
Discrimination and Compelled Disclosures

Discrimination and Compelled Disclosures

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:



Discrimination and Compelled Disclosures*

Purpose: Recent **Connecting for Health** public opinion research found that more than half of respondents were “very concerned” that employers or health plans would gain access to electronic information intended for PHRs.¹ Worry about possible employment or insurance discrimination likely drives these high numbers.

CT1: Technical Overview discusses “business data streams” and “consumer data streams.” Business data streams consist of transactions of personal health information among business partners conducted without a consumer view or participation. For example, consumers generally don’t see the transactions between their doctor’s office and the insurance company, or between the insurance company and its data warehouse, etc. Consumer data streams involve transactions of information into or out of a consumer-accessible application, such as a PHR.

In addition to the enforcement of existing anti-discrimination laws, any organization acting as Consumer Access Service or PHR supplier should maintain a “firewall” between consumer data streams and business data streams to ensure that data captured or stored in consumer applications are not used as a basis for discrimination.

Our Work Group recommends that all network participants treat consumer data streams distinctly — with higher levels of

* **Connecting for Health** thanks 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.

¹ 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 the following URL: http://www.markle.org/downloadable_assets/research_doc_120706.pdf.

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

4. Use limitation

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.

protection than existing business streams of health data. This practice area recommends tough language to bar discrimination or “compelled disclosures” — such as when the consumer’s authorization for release of data is required in order to obtain employment, benefits, or other services.

Discrimination

It is important to recognize that consumer data streams and networked PHRs may lead to a commingling or at least co-existence of data from a variety of sources, including the consumer. It would threaten the consumer’s trust in the entire network if the PHR were used as the source of information, no matter its origin, that affected an underwriting or employment decision. The **Connecting for Health** Common Framework policies for health information exchanges prohibit use of information for discriminatory purposes.² Similarly, employer groups have publicly stated that they will never access individually identifiable information generated and stored in the PHR services that they offer to their employees.

² **Connecting for Health** Common Framework, *Model Privacy Policies and Procedures for Health Information Exchange*. June 2006, p. 10-11. Available online at: http://www.connectingforhealth.org/commonframework/docs/P2_Model_PrivPol.pdf.

Recommended Practice:

The preferred practice is to guarantee that none of the information made accessible to or from the consumer's application — that is, none of the consumer data stream — can ever be used to discriminate against consumers. In addition to complying with all anti-discrimination laws and regulations, all entities that access information in a consumer data stream should make public statements, and develop internal practices against using information in consumer data streams for purposes of discrimination. When appropriate, Consumer Access Services and PHRs should include anti-discrimination clauses in their contracts with partners. The best means of preventing information from being used for discrimination is to put in place strong policies and access control procedures.

It is noted that some organizations, particularly HIPAA-Covered Entities such as health plans and self-insured employers, collect personal health information to perform their business operations (i.e., as part of the business data stream) as well as offer Consumer Access Services. In addition to complying with all anti-discrimination laws and regulations, such organizations should use prudent practices such as implementing a "firewall" between consumer data streams and business data streams in order to prevent even the appearance of being able to use information in consumer data streams for purposes of discrimination.

Compelled Disclosures

According to the chair of the Subcommittee on Privacy and Confidentiality of the National Committee on Vital and Health Statistics: "Each year, as a condition of applying for employment, insurance, loans, and other programs, millions of individuals are compelled to sign authorizations permitting employers, insurers, banks, and others to access their personal health information for non-medical purposes. These authorizations are nominally voluntary; individuals are not required to sign them, but if they do not, they will not be considered for the particular job, insurance policy, loan, or benefit. In addition, for most of these authorizations, no

limits are placed on the scope of the information disclosed or the duration of the authorization."³

Few laws or regulations place limits on such compelled disclosures. To date, most information released under such circumstances comes from what we call business data streams, e.g., from official medical records, etc.

If consumer data streams and PHRs are opened to such compelled authorizations, it will seriously undermine the public confidence in these new tools. If consumers fear that information in their networked PHR must be released to third parties considering their applications for employment, benefits, loans, etc., many will avoid health information services that might otherwise help them manage their health.

Recommended Practice:

Absent statutory protection from compelled disclosures, the emerging industry of Consumer Access Services should take a strong public and legal stand against third parties seeking to make their own access to consumer data streams and networked PHR information a condition of an individual's employment, benefits, or other services important to the well-being of individuals.

³ Rothstein, Mark, June 2006 Letter to HHS Secretary Leavitt. Accessed online on October 9, 2007, at the following URL: <http://www.ncvhs.hhs.gov/060622lt.htm>. See also *Compelled Disclosure of Health Information: Protecting Against the Greatest Potential Threat to Privacy*. JAMA, Volume 295(24), 28 June 2006, p. 2882-2885.

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)

Joyce Dubow, AARP

Thomas Eberle, MD, Intel Corporation and Dossia

Staff

Matt Kavanagh, Independent Contractor
Josh Lemieux, Markle Foundation

Lisa Fenichel, Health Care For All

Stefanie Fenton, Intuit, Inc.

Members

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

Steven Findlay, Consumers Union

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

Annette Bar-Cohen, MPH, National Breast Cancer Coalition

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

Jeremy Coote, InterComponentWare, Inc.

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

Maureen Costello, Ingenix

Diane Davies, MD, University of Minnesota

James Dempsey, JD, Center for Democracy and Technology

Philip T. Hagen, MD, Mayo Clinic Health Solutions

Stephen Downs, SM, Robert Wood Johnson Foundation

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.*