CP1 CP2 CP3 CP4 CP5 CP6 CP7 CP8 CP9

CT1 CT2 CT3 CT4 CT5 CT6 CT7

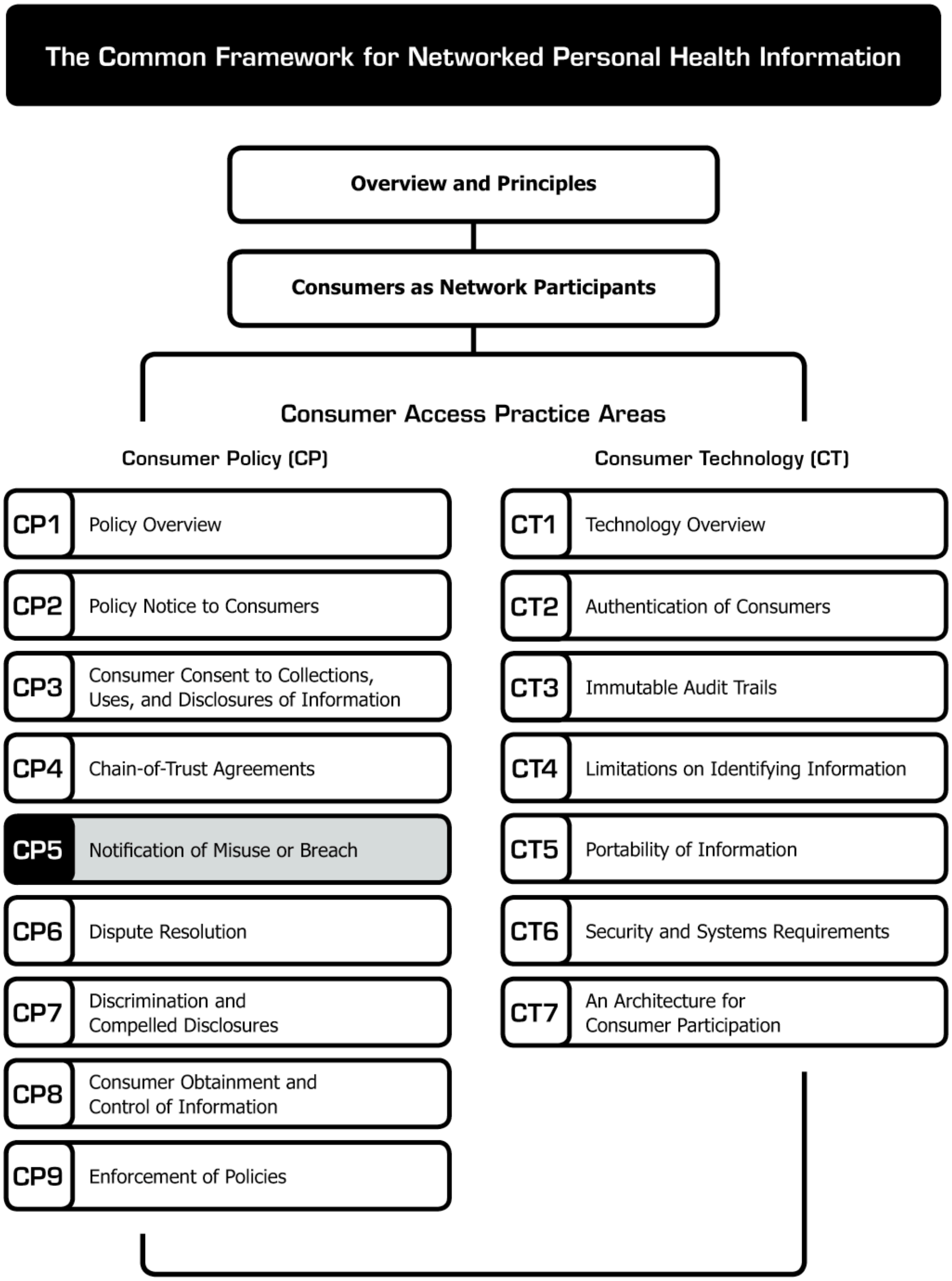
Notification of Misuse or Breach

Notification of Misuse or Breach

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:



The Common Framework for Networked Personal Health Information

Overview and Principles

Consumers as Network Participants

Consumer Access Practice Areas

Consumer Policy (CP)

- CP1 Policy Overview
- CP2 Policy Notice to Consumers
- CP3 Consumer Consent to Collections, Uses, and Disclosures of Information
- CP4 Chain-of-Trust Agreements
- CP5 Notification of Misuse or Breach
- CP6 Dispute Resolution
- CP7 Discrimination and Compelled Disclosures
- CP8 Consumer Obtainment and Control of Information
- CP9 Enforcement of Policies

Consumer Technology (CT)

- CT1 Technology Overview
- CT2 Authentication of Consumers
- CT3 Immutable Audit Trails
- CT4 Limitations on Identifying Information
- CT5 Portability of Information
- CT6 Security and Systems Requirements
- CT7 An Architecture for Consumer Participation

Notification of Misuse or Breach [*]

Purpose: Secure and confidential data handling is a core responsibility for any Consumer Access Service. Part of this responsibility includes developing an advance plan on what the Consumer Access Service will do if something goes wrong. There have been many highly publicized inadvertent disclosures of sensitive personal data.

Our review of leading PHRs revealed a widespread lack of policy statements about responsibilities and actions that the company will take in the event of a breach or misuse of personal health information. (*See* ***Appendix A of CP2: Policy Notice to Consumers***.)

California is the leader among several states that have enacted laws requiring companies to notify affected consumers when sensitive, personally identifiable data are disclosed into unauthorized hands, but such requirements are not yet universal.[1] Notification regarding health data breaches is controversial and subject to debate. Open questions include, for instance, what constitutes a breach? What types of data are at issue? What constitutes notice?

We recommend that Consumer Access Services develop policies for breach or misuse of information. Such policies should be posted as part of the part of the publicly available notice of privacy and security policies. (*See* ***CP2: Policy Notice to Consumers***.) Notwithstanding the lack of guidance or industry acceptance, Consumer Access Service policies should notify users of what the service believes to be a significant breach, how it will notify users when a breach occurs, and what recourse the user has in the event of a breach.

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

5. Individual participation and control

7. Security safeguards and controls

8. Accountability and oversight

9. Remedies

* "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.

Recommended Practice:

A Consumer Access Service should notify individually any user whose 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.

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

[1] The Privacy Commissioner of Canada has a helpful resource, *Overview of American Breach Notification Laws*. February 22, 2007. Accessed online on August 22, 2007, at the following URL: http://www.privcom.gc.ca/parl/2007/sub_070222_06_e.asp.

The notification should be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Notification practices should be consistent with state-of-the-art security standards and should be "risk-based" — tailored to the potential risk to the consumer and the size, complexity, and nature of the Consumer Access Service's operations. A current "best practice" for notification is described by the California Department of Consumer Affairs.[2]

[2] California Department of Consumer Affairs, *Recommended Practices on Notice of Security Breach Involving Personal Information*. February 2007. Accessed online on September 6, 2007, at the following URL: http://www.privacyprotection.ca.gov/recommendations/secbreach.pdf.

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.*