CP1 CP2 CP3 **CP4** CP5 CP6 CP7 CP8 CP9

CT1 CT2 CT3 CT4 CT5 CT6 CT7

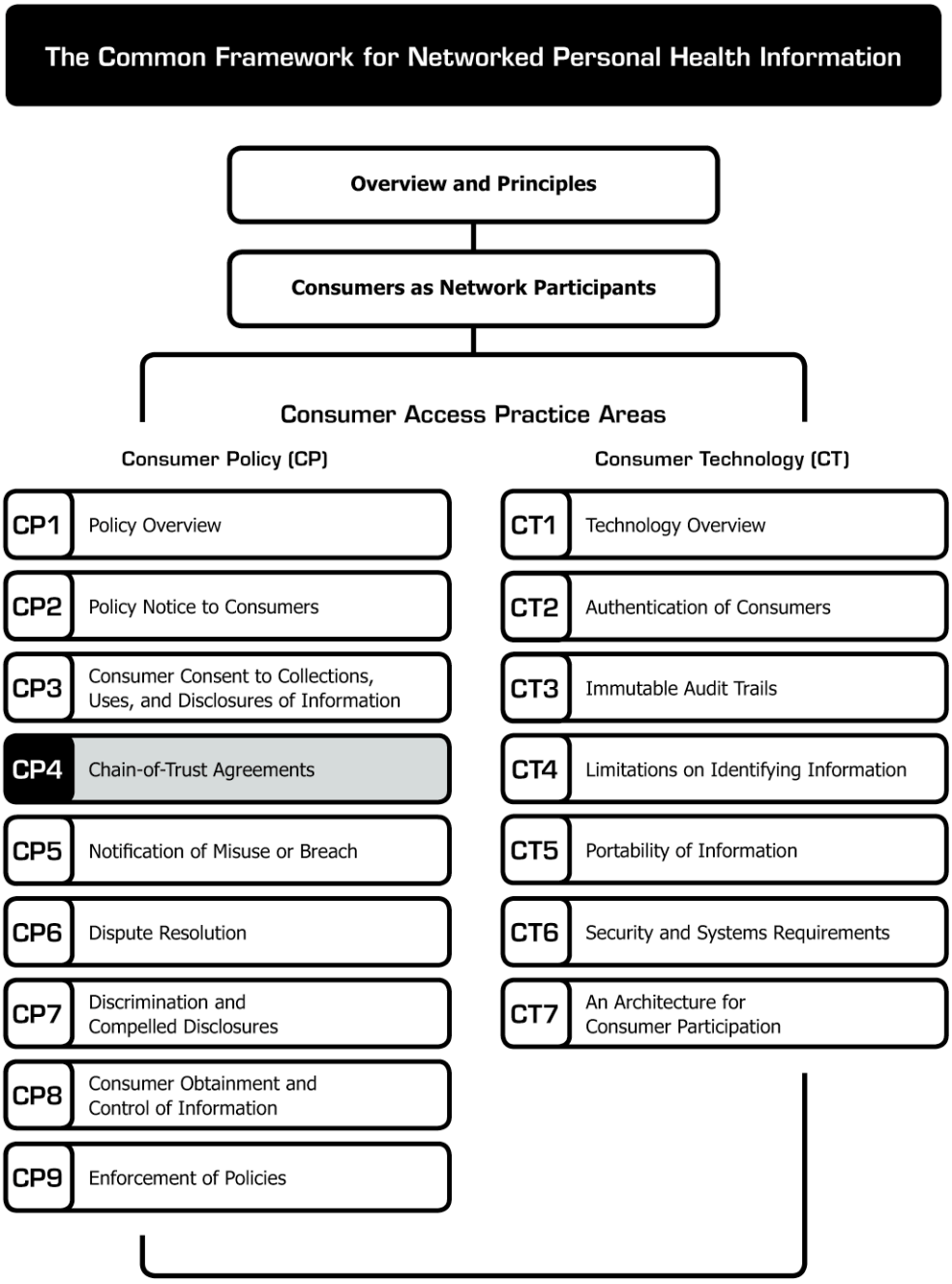
Chain-of-Trust Agreements

Chain-of-Trust Agreements

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:



Chain-of-Trust Agreements*

Purpose: For personal health information to flow in or out of a consumer-accessible application, it may pass among two or more organizations. Each participant in such "consumer data streams" may have its own legal and business interests to protect. However, consumers should be able to trust the entire chain of entities and business processes that handle their personal health data. Contracts are one mechanism to bind partners to specified privacy and security policies regarding confidential information they exchange or share.

Like other policy areas in this framework, chain-of-trust agreements are often necessary in certain relationships, but not by themselves sufficient to create a privacy-protective environment. In practice, such contracts have significant weaknesses, including their lack of transparency to consumers and their inconsistent enforcement. For one, breaches may not be discovered because organizations may not rigorously monitor the behavior of all of their business partners. Secondly, if an accusation of breach occurs, enforcement depends on one party engaging another party in a legal action, most likely under contract law. Organizations often seek to settle legal disputes out of court — or avoid litigation altogether.

Still, chain-of-trust agreements serve as important instruments in encouraging "good network citizenship." There are several possible relationships in which parties seek chain-of-trust agreements. HIPAA Business Associate agreements are one example. *(See **CP1: Policy Overview**.)*

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

8. Accountability and oversight

* "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.

There is a problem with scaling this chain-of-trust model, however. It is unreasonable, for example, for each doctor's office to negotiate and sign a chain-of-trust agreement with every Consumer Access Service or networked PHR provider. Instead of each participant signing agreements with each other participant, it may be more practical if all participants agreed to a basic set of "network rules" — a set of common practices that each participant would sign and publicly commit to uphold. Although there are no such large-scale arrangements for Consumer Access Services or PHRs today, such models should be explored.

The HIPAA regulations permit consumers to request their personal health information directly from Covered Entities. Consumers may then store the information with any Consumer Access Service of their choice. In this case, the Consumer Access Service does not need a chain-of-trust agreement with the Covered Entity. The consent agreement(s) between the consumer and the Consumer Access Service should spell out the information-handling practices of the Consumer Access Service. (*See **CP4: Consumer Consent to Collections, Uses, and Disclosures of Information**.*)

A Consumer Access Service may not be regulated under HIPAA, and it may have unregulated relationships with many different types of third parties. In such cases, chain-of-trust agreements between the Consumer Access Service and its third parties are a prudent mechanism to discourage unacceptable actions. Such agreements should prohibit activities that

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

are inconsistent with fair information practice principles, such as the surreptitious re-identification of de-identified data without the consumer's knowledge or consent. The recommended practice language below is primarily intended for this scenario (i.e., an uncovered Consumer Access Service's relationship with unrelated and unregulated third parties), but it may be helpful in other relationships as well.

Recommended Practice:

Consumer Access Services should contractually bind third parties with which they share or exchange personally identifiable, partially identifying, and de-identified data to:

- Prohibit unauthorized use and disclosure of such data.
- Protect the data in accordance with policies and authorizations agreed to by the consumer, when applicable.
- Prohibit unauthorized attempts to identify de-identified data by, among other things, combining it with other databases of information. (*See **CT4: Limitations on Identifying Information** for a discussion of personally identifiable, partially identifying, and "de-identified" data*.)
- Notify the Consumer Access Service if the third party is aware of a breach or misuse of information in a form that carries significant risk of compromising the security, confidentiality or integrity of personal information. (*See **CP5: Notification of Misuse or Breach***.)

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.*