CP1 CP2 CP3 CP4 CP5 CP6 CP7 CP8 CP9

CT1 CT2 **CT3** CT4 CT5 CT6 CT7

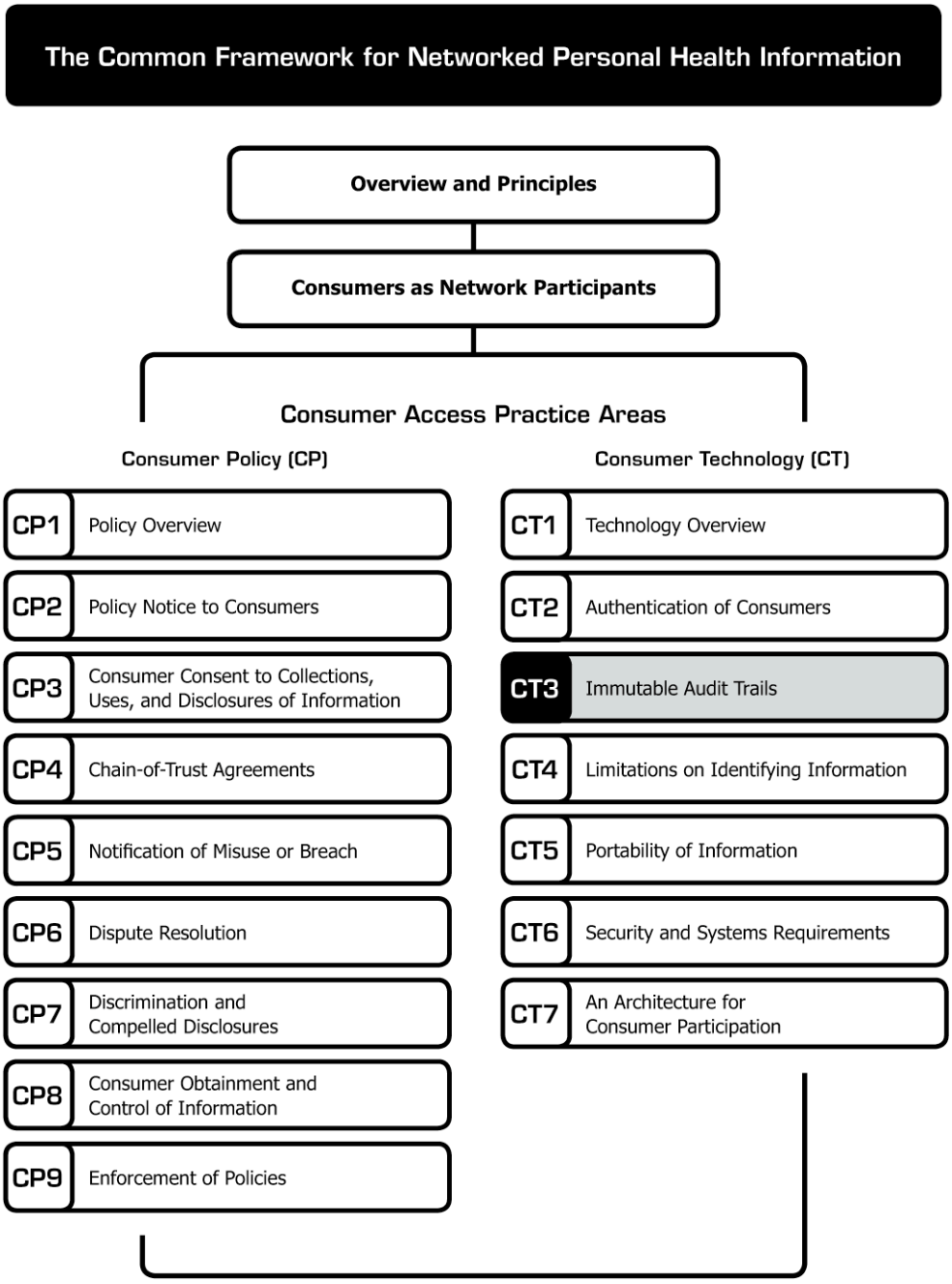
Immutable Audit Trails

Immutable Audit Trails

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:



Immutable Audit Trails*

Purpose: Audit trails are a basic requirement for electronic health information in EHRs and PHRs. Consumer Access Services must provide consumers with convenient electronic access to an audit trail as a mechanism to demonstrate compliance with use and disclosure authorization(s). An audit trail as defined here is an easy-to-comprehend date-, time-, and source-stamped historical record of significant activities and transactions that pertain to access of the consumer's account and the use and disclosure of personal data within. Of note, electronic audit trails have been in wide use in Internet banking; a 2004 survey found that almost all banks provide joint account holders with a clear audit trail that details which account holder performed which transaction.[1]

The audit trail compiled and maintained by a Consumer Access Service should be the same audit trail displayed to the consumer, and each audit trail entry should be immutable (i.e., unchanging and unchangeable) in content.

Persistence of the audit trail should be commensurate with the data persistence policies of the Consumer Access Service. For example, if the Consumer Access Service retains professionally sourced data for seven years, then entries in the consumer's audit trail should persist for at least this same period of time.

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

4. Use limitation

5. Individual participation and control

6. Data quality and integrity

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.

Source-stamping is particularly important for end-users to evaluate the validity of information displayed from a consumer data stream. There are cases when a given data element may have more than one "source." For example, consider the case in which a Consumer Access Service is authorized to obtain the previous 90 days of prescription medication history on the consumer's behalf from a retail pharmacy clearinghouse. When the information is imported into the consumer's application, the clearinghouse is a "source" of the transaction. Upstream of that transaction, there were other "sources," like the doctor who wrote the prescription and the pharmacy that filled it. Ideally, the audit history should include each relevant upstream and downstream source. Consumer-sourced entries must be marked as such.

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

[1] American Bankers Association, Summary of Survey on Internet Banking: Online Enrollment, Account Opening, and Fraud Prevention. May 2004. Accessed online on August 28, 2007, at the following URL: http://www.aba.com/NR/rdonlyres/C38C00C0-071B-4944-904B FC4A734CBC7F/35916/InternetSummary2004.pdf.

Recommended Practice:
Each Consumer Access Service should maintain an easy-to-comprehend and clearly labeled electronic audit trail containing immutable entries that pertain to the consumer's account, information, and policy consent. Each entry should identify, at a minimum, who has accessed the consumer's records, a date, time, and source stamp for each such access, and the source of each significant transaction. The audit trail should be retained at minimum according to the data retention practice of the service.

We suggest the following as "auditable" events/activities:

1. **Account:**
    a. Access attempts and outcomes (i.e., successes or failures, length of session), including those by proxies.
    b. Logout events, including those by proxies.

2. **Transactions and data:**
    a. Creation (e.g., self-reported allergy)
    b. Modification (e.g., self-reported downward adjustment to a medication's dosage frequency)
    c. View (e.g., access of a problem list)
    d. Export (e.g., export of data to a PDA or spreadsheet)
    e. Import (e.g., import of data from a claims clearinghouse)
    f. Deletion (e.g., removal of a medication the consumer no longer takes)
    g. Dispute (e.g., the consumer challenges the accuracy of a professionally sourced data element)
    h. Proxy (e.g., setting up access to the record by a proxy, such as a caregiver)

3. **Policy:**
    a. Consent (e.g., capture of the consumer's general and independent consents, with roll-back access to versions of applicable policies to which the consumer consented)
    b. Revocation (e.g., the consumer decides to terminate a previously authorized consent that allowed sharing of data with a 3rd-party service provider)

*(For related information, see **CP8: Consumer Obtainment and Control of Information, Proxy Access.**)*

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.*