CP1 CP2 CP3 CP4 CP5 CP6 CP7 CP8 CP9

CT1 CT2 CT3 CT4 CT5 **CT6** CT7

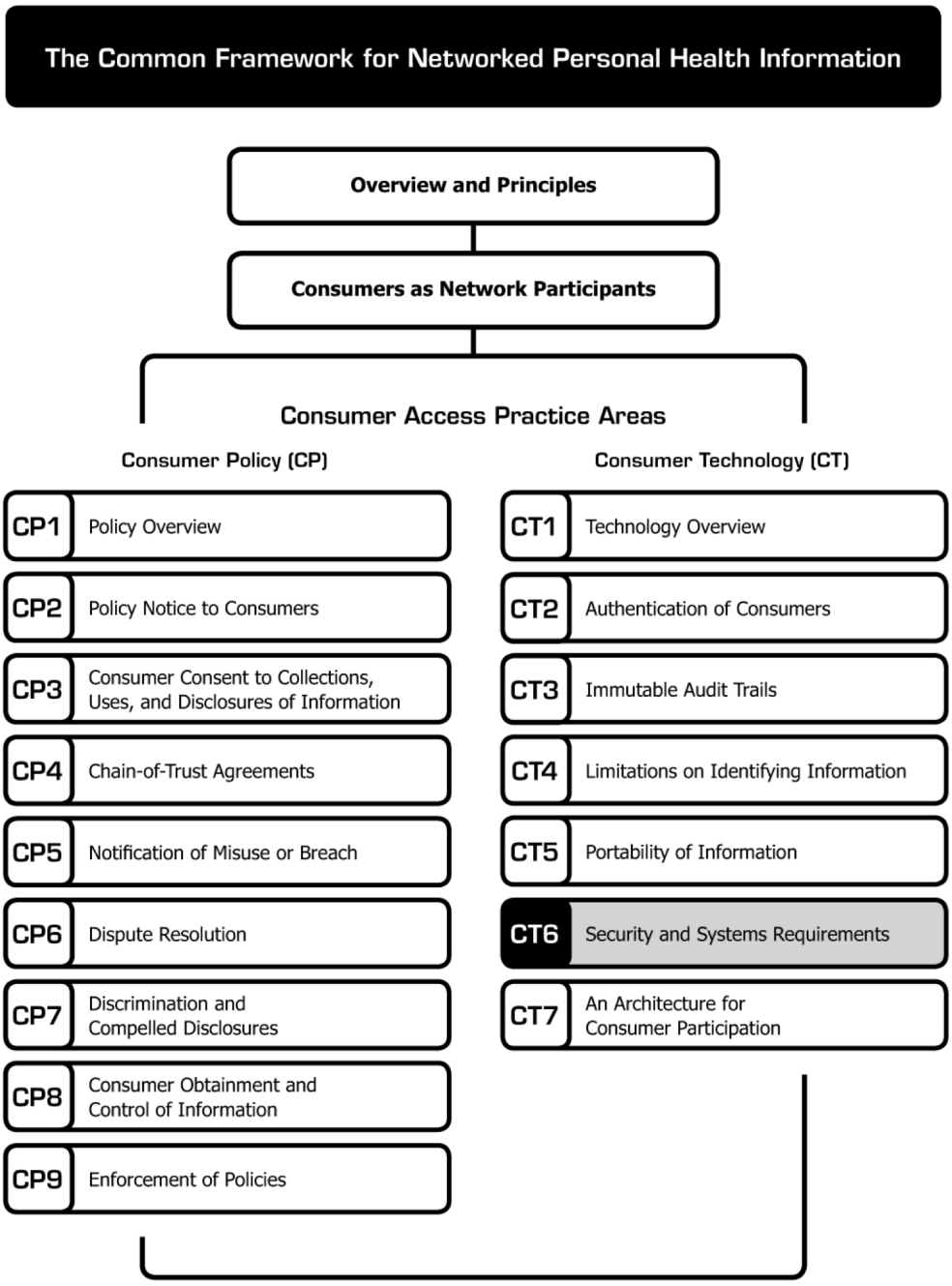
# Security and Systems Requirements

# Security and Systems Requirements

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:



# Security and Systems Requirements*

**Purpose:** Strong security and systems requirements are essential to maintain trust among all network participants handling personal health information. Without such protections, consumer adoption will likely be hampered out of concern about the security of their data,[1] and Health Data Sources may continue to view the release of consumer data to Consumer Access Services as too great of a privacy risk to implement.[2] Although this practice area notes the need for strong security, detailed recommendations are beyond the scope of this paper. The HIPAA Security Rule is a good starting point. Another valuable reference is the government's recommended security protocols for federal information systems.[3] Below, we outline a few basic security considerations:

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

**7. Security safeguards and controls**

* "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.

## Data Stores

- Facilities that house equipment (e.g., servers, backup devices, etc.) that store health data must be physically secured and attended at all times. Access to such equipment should be limited to individuals who require it for authorized, legitimate, and documented (i.e., auditable) purposes.
- Individuals who access user data may only access the minimum amount of data necessary to fulfill their authorized purpose(s).
- Sensitive user data should be encrypted within the equipment that holds the data so as to prevent unauthorized access and disclosure in the case of a physical loss.
- Because most security breaches occur from within an organization (whether intentional or not), it is important to require that all persons who have access to such data receive regular training and appropriate reminders about system security and the need to follow related protocols to protect the confidentiality of user information. In addition, policies should be in place (and regularly communicated) to handle persons who violate stated security protocols.
- Strong system security for Consumer Access Services and networked PHRs also entails regular risk assessments and system audits.

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



1 Win, Susilo, Journal of Medical Systems, *Personal Health Record Systems and Their Security Protection*. 30:4, p. 309-315, August 18, 2006.

2 R. Lecker et al., *Review of the Personal Health Record (PHR) Service Provider Market*. March 14, 2007 (http://www.hhs.gov/healthit/ahic/materials/05_07/ce/chin.html, "2.4.2.2 Interoperability Challenges").

3 NIST Special Publication 800-53, Revision 1, National Institute of Standards and Technology, *Recommended Security Controls for Federal Information Systems*. December 2006. Accessed online on May14, 2008, at the following URL: http://csrc.ncsl.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf.

## Transactions

- When information is presented to a user's web browser from equipment that holds this data (i.e., a data server), all reasonable steps should be taken to ensure a secure transmission of the user's data, including use of encryption protocols such as Secure Socket Layer (SSL) technology.
- Consumer Access Services should comply with industry best practices for transmission of health data over the Internet even if they are not subject to information security regulations governing the health care industry.

The following are other considerations in the emerging PHR industry:

- In addition to data storage and transactional security, it is also important to apply security and systems requirements to electronic mobile storage devices such as smart cards, memory sticks, and mobile devices offered as consumer access platforms and/or data portability options (Note that security requirements applicable to mobile storage devices that hold personal health data should be in place not only for the benefit of the consumer, but also for the benefit of care providers who may wish to connect the device to their own computer and/or network in order to access and/or update a user's health information.) Without strong security and systems requirements guaranteeing protection, the benefit these devices may offer to care providers may be outweighed by the security threat posed by viruses, trojan horses, or other malware that may be "hiding" within.[4]

***Recommended Practice:***

Consumer Access Services should adopt industry best practices for data transaction and storage security. Security requires continuous monitoring of industry practices and threats, as well as initial and ongoing personnel training and strict policies regarding who can access consumer data, limitations on data that can be accessed by authorized purpose, and consequences of and for security violations. Services will need to adapt to emerging practices to ensure the security of information entrusted to them, with special attention to additional protections for sensitive data. Services must be accountable for export and storage of information in applications that they have endorsed, whether those applications are browser-based or mobile devices.

[4] Sittig and Wright, *USB Flash Drives Pose Threat To Health Care Provider Computer Systems*. February 20, 2007. Accessed online on August 28, 2007, at the following URL: http://www.ohsu.edu/ohsuedu/newspub/releases/022007flash.cfm.

## 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.*