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

CT1 CT2 CT3 CT4 CT5 CT6 CT7

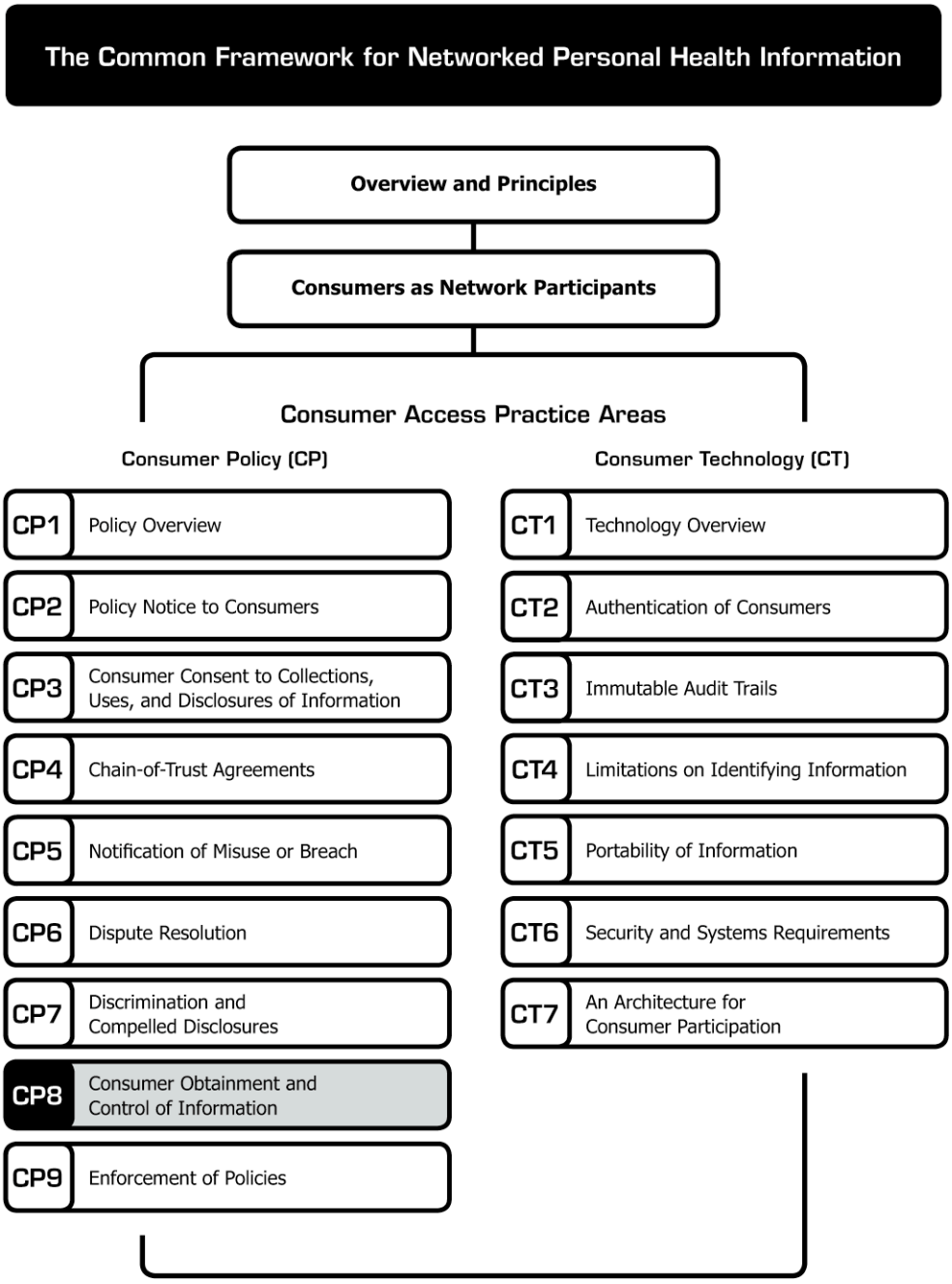
Consumer Obtainment and Control of Information

Consumer Obtainment and Control of Information

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:



Consumer Obtainment and Control of Information*

Purpose: Opinion surveys reveal that most Americans want to be able to get electronic copies of their health information.[1] Generally, business data streams in health care provide consumers with few opportunities to control the flow of their data, particularly when third party payers are involved. (*See* ***CT1: Technology Overview***.) In contrast, consumer obtainment and control are the core attributes of the copies of data that flow into and out of PHRs.[2]

There is a substantial range of views about what constitutes "control" for consumers. Some clinicians worry about the reliability of consumer-sourced information, or are concerned that consumers might withhold or alter their records in a way that ultimately compromises their care. It is useful to reiterate three concepts that recur throughout this paper:

- **Copies:** Separate sets of copies can be controlled individually. If a consumer imports a copy of her information into a PHR, it does not mean that she will control the same information held at the original source. She controls only her copy.
- **Distinction between PHR and EHR:** PHRs are not a replacement for the record-keeping responsibilities of clinicians or other health entities. (See *Health Application Terminology on page 2*.)
- **"Source of truth":** In a networked health information environment, various data holders, including consumers, keep multiple copies of health data. There is no default "source of truth." Every piece of information must be evaluated based on many factors, including its source. Whether a patient fills out a clinical intake questionnaire, answers questions orally in the examining room, or transmits information from a PHR, the attending clinicians must make judgments about the completeness and validity of the information. (Intentionally or not, consumers have always had the ability to withhold or misrepresent information via any of these methods.) Similarly, patients cannot take for granted the completeness or accuracy of information held about them by the health professionals providing their care. (In fact, providing consumers with access to copies of the information about them can help all parties improve the accuracy and completeness of the information they hold.) A critical component of assessing the validity of information in an electronic environment is the automated electronic time-, date-, and source-

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

5. Individual participation and control

6. Data quality and integrity

* "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.

---

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

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. See also the results of a Harris Poll, March 26, 2007, accessed online on August 29, 2007, at the following URL: http://www.harrisinteractive.com/harris_poll/index.asp?PID=743.

2 The ideal attributes of a PHR are described in the **Connecting for Health** paper, *The Personal Health Working Group: Final Report*. 2003, page 16. Accessible online at: http://www.connectingforhealth.org/resources/final_phwg_report1.pdf.

Health Application Terminology

The term "personal health records" is inadequate because of its emphasis on "records" as past information. To make sense of their health and health care, consumers likely want useful tools and convenient services more than mere records. Some prefer the term "personal health applications." However, we use the term PHR because it has become a term of art. Below are the broad definitions we use for the applications used by health consumers and clinicians:

Personal Health Records (PHRs) encompass a wide variety of applications that enable individuals to collect, view, manage, or share their health information and conduct health-related transactions electronically. Although there are many variants, PHRs are intended to facilitate an individual's ability to bring together (or designate others to help them bring together) their personal health information into an application that the individual (or a designee) controls. PHRs may contain data developed and managed by health-related institutions as well as information developed by the individual.

Electronic Health Records (EHRs) are different from PHRs in that they are used by clinicians rather than consumers and patients. EHRs are designed to replace and improve upon the paper patient "chart." We do not envision PHRs as a substitute for the professional and legal obligation for recordkeeping by health care professionals and entities.

stamping of all data transactions, and all data entries in PHRs and EHRs. (*See* ***CT3: Immutable Audit Trails***.) This paper identifies six dimensions of consumer access and control in a networked PHR environment. The specific levels of consumer control may vary depending on the type of the Consumer Access Service and/or the PHR application in use.[3] The following discussion recommends general practices and identifies areas that require further collaborative definition.

Area 1: Consumer Requests for Personal Health Information in Electronic Format

Consumers should have a convenient means to request electronic copies of their information from health data sources. We recommend that stakeholders work on a standard electronic messaging "envelope" for consumers to authorize health data sources to exchange electronic copies of their health information with Consumer Access Services of the consumers choosing, plus standard protocols for reliably routing such requests and authorizations. The concept is similar to online banking, in which consumers can download transaction histories in industry-standard formats from their multiple financial institutions into applications they control on their desktop computers.[4]

Recommended Practice:

Consumer Access Services should facilitate convenient access for consumers to obtain copies of their personal health data in electronic formats. Requests on behalf of a consumer to obtain electronic copies of information about the consumer from Health Data Sources must be explicitly authorized by the consumer, and should conform to standard formats and protocols as such standards and protocols become available.

[3] Some PHRs are provided directly by health care providers, providing consumers with view-only data from the institutional electronic health record. These may provide consumers with no functionality to append, alter, or delete information. Other PHRs may provide higher levels of consumer control, but fewer opportunities to share the information electronically with clinicians. A previous **Connecting for Health** Work Group explored issues related to the consumer's ability to amend, append, or withhold data in PHRs. See *Connecting Americans to Their Health Care: Work Group on Policies for Electronic Information Sharing Between Doctors and Patients*, Markle Foundation, July 2004, p. 84-88. Available online at the following URL: http://www.connectingforhealth.org/resources/wg_eis_final_report_0704.pdf.

[4] Work to define such a standard should consider, among other things, the lessons learned from the development of Open Financial Exchange (OFX) — an industry standard for consumer and small business online banking, bill payment, bill presentment, investment transaction download, and 401(k) account access. For technical information, see http://www.ofx.net/.

Area 2: Proxy Access to Account

It is generally agreed that PHRs should enable an individual account holder to designate someone else, such as a family member, care provider, caregiver, or legal guardian, to act on the account holder's behalf. Proxy permissions can vary depending on the individual account holder preferences and the role of the proxies. It goes beyond the scope of this paper to explore the application-level functionality of designating such permissions in detail.

The required policies involve complex tradeoffs, particularly where minor children may have health issues they'd prefer be kept private, but lack legal authority to block proxy access to their information (state laws and local practices vary widely in this regard), or where grown children are handling the health information or setting up an account for incapacitated parents. A proxy access protocol that may work well in one family context could be overly revealing or obstructive in a different household.

Similarly, appropriate proxy access protocols will necessarily vary depending, for example, upon whether the proxy is a lay guardian or caregiver, whether the individual is capable of designating a proxy, whether the proxy is initiating an account for a dependent child or parent, whether there is a special use case such as an unconscious patient in an emergency room, etc. Because these issues require deliberation beyond the scope of our Work Group, we offer only general recommendations:

Recommended Practice:

The consumer's ability to designate proxy access should be as specific as feasible regarding:

- Authorization to data (such as read-only, write-only, read/write, or read/write/edit).
- Access to data types (e.g., access to all information, access only to medications, etc.)
- Access to functions (e.g., send a message to a provider, grant/revoke proxy access to someone else, etc.), when appropriate.
- Role permissions (e.g., health professionals, elective proxies selected by consumer, legal proxies determined by law such as parents or guardians of minors).
- Ability to further designate proxies (e.g., can those serving as proxies designate others as proxies?)

In addition, proxy access should be:

- Subject to the granting of separate authentication and/or login processes for proxies.
- Tracked in immutable audit logs designating each specific proxy access and major activities. (*See* ***CT3: Immutable Audit Trails***.)
- Time-limited and easily revocable.

(Note: Time-limiting or revoking proxy access is typically on a "going-forward" basis; it will not "recall" information previously obtained and copied by a proxy. Example: A consumer named Millie provides proxy access to her caregiver and her doctor, then later revokes it. Both proxies had made electronic copies of Millie's information into their own systems during the time they had legitimate access to Millie's information. Millie's act of revoking proxy access does not mean that the information her caregiver or her doctor obtained is somehow automatically "erased" or "withdrawn" from their systems. Those former proxies may keep or erase the copies of Millie's information depending on the proxies own policies and obligations under which they obtained the information. In this example, the doctor's obligation to retain information may differ substantially from those of the caregiver.) (*See* ***Area 4: Retention of Information*** *below*.)

Area 3: Requests to Amend or Dispute Entries

Under HIPAA, consumers have the right to request that information be added to their health data held by Covered Entities to make it more accurate or complete. Consumer Access Services, whether HIPAA-covered or not, have the potential to engage consumers in the essential and never-ending effort to improve data quality across the health sector. We recommend a multi-stakeholder effort to define a standard messaging envelope and markup language for consumers to request amendments or dispute entries to their information obtained through consumer data streams.

To the extent feasible, Consumer Access Services can facilitate the routing of such requests back to health data sources. This

practice area concerns only information that is professionally sourced (e.g., from a doctor's office, hospital, lab, pharmacy, payer, etc.) We presume that consumers will be able to edit or delete their own data entries at will.

Recommended Practice:
Users should be able to identify any errors or omissions in the posted information and be afforded a process to communicate requests for changes back to the original source of information.

A Consumer Access Service should provide notice to users as to whether a request to modify a record requires that the user submit a request to the Consumer Access Service, or directly to the appropriate Health Data Source. If the former, the Consumer Access Service should provide an easy and convenient method for the consumer to request corrections. If the latter, the Consumer Access Service should notify the user that he needs to contact the Health Data Source directly. Ideally, the Consumer Access Service should provide information about how the user can contact the original source(s) of information that the consumer believes to be in need or amendment (e.g., the original source's customer service 1-800 number).

Consumer Access Services should provide mechanisms to route data correction requests and responses between consumers and Health Data Sources electronically as standards and protocols for such requests and responses become widely available. Ideally, such standard messages will include:

- Consumer request for emendation or removal of data.
- Response back from Health Data Source confirming concurrence with request or reason for denial of request.
- Consumer's dispute of data not changed, to be appended to data in question.

Area 4: Retention of Health Information

Statutes vary from state to state regarding the time that medical professionals are required to retain patient information. The average requirement for record retention is 5 to 7 years after the patient has last visited, although some states require data retention much longer. Information maintained in Consumer Access Services offered by health professionals or health care facilities may be subject to such laws. Many Consumer Access Services, however, are not offered by regulated health care professionals or facilities, and therefore generally are not subject to these state record retention requirements. In fact, there are no clear general guidelines for how long unregulated entities should store health information on behalf of consumers.

Our Work Group does not propose a general standard for a minimum or maximum time that a Consumer Access Service or PHR should retain information in an inactive consumer account. The participants did agree, however, that Consumer Access Services:

- Should provide adequate notice of their data-retention policies.
- Should retain information based on its specified purpose(s), and information should not be retained once its purpose(s) is completed.
- Should attempt to alert consumers before their records are scheduled to be deleted or made inaccessible, and should provide mechanisms for consumers to copy their information prior to it being deleted or made inaccessible. (*See* ***CT5: Portability of Information***.)
- Should tailor data-retention policies according to their specific relationship with consumers. For example, a HIPAA-Covered Entity offering Consumer Access Services may wish to match its own record-retention policies as guided by state laws; whereas a subscription-based service offered by an uncovered entity may establish relationships based on shorter data persistence unless actively renewed by the consumer.
- Should reduce the risk of re-identification of individuals by, among other things, limiting the duration of storage of passively generated information that is not intended to be part of the consumer's longitudinal health record (e.g., IP addresses, cookies, and web beacons).

Recommended Practice:
For organizations authorized by the consumer to store information as part of a consumer data stream, the data-retention practices of Consumer Access Services should be transparent to the consumer. Such practices should be part of the notice of policies. (*See* ***CP2: Policy Notice to Consumers***). Consumer Access Services and networked PHRs should develop and communicate unambiguous policies regarding the persistence of information they hold on behalf of consumers. Such policies should be based on the principles of purpose specification, use limitation, and data minimization. That is, information should be retained based on its authorized purpose(s), and not retained after such purpose(s) are completed.

For inactive accounts, preferred practices may include sending notices to the consumer, providing the consumer with the option to renew or extend the retention period, or to close out the account. Should the consumer fail to respond to such notices, there should be at least one notice shortly prior to the expiration of the data-retention period, explaining that the account will be rendered inactive as of its end date unless the consumer takes action to extend it.

To reduce the risk of re-identification of individuals, Consumer Access Services and PHRs should retain passively generated information that can be used to re-identify individuals (IP addresses, cookies, and web beacons) for shorter periods than information that is actively provided by the consumer or authorized Health Data Sources as part of a longitudinal health record. (*See* ***CT4: Limitations on Identifying Information*** *for a more detailed discussion of this issue*.)

Area 5: Expunging of Information

There are two circumstances in which information held by a Consumer Access Service on behalf of a consumer may be expunged:

1. According to the Consumer Access Service's publicly available data retention practices (i.e., upon the end date of the consumer's inactive account data retention period), and,
2. Upon request by the consumer, at any time during her relationship with the Consumer Access Service, including upon termination of account (see below).

By expunging, we mean rendering the information inaccessible from live servers if not deleting it outright, and storing any remaining information in ways that make it unable to be reconstructed in an individually identifying manner. Because reasonable consumers are often unaware that information that they "delete" within their own applications may often persist in other data stores or caches, it is vital that the end result of the "expunging" activity be clearly stated and transparent. We anticipate that expunging will often occur in conjunction with requests to terminate an account.

Recommended Practice:
Consumer Access Services should provide a mechanism for their users to request expunging (as defined above) the information held in their accounts. To the extent feasible, a Consumer Access Service should enable consumers to request expunging of information in whole or in part. Upon request by the consumer to expunge information, the Consumer Access Service should provide a mechanism for consumers to make copies of their information to the extent feasible. (*See* ***CT5: Portability of Information***.) Once the consumer has confirmed a request to expunge information, the Consumer Access Service should carry out such action without delay and within a reasonable timeframe.

Consumer Access Services should provide the requesting consumer with timely notice of the status of requests for account termination and/or expunging of information. Such notice of status should clearly state the consequences and actual definition of "expunging" of information.

Regarding requests for expunging of information, the Consumer Access Service should delete the information to the extent feasible and, absent full deletion, at a minimum render the information inaccessible from live servers and take care to ensure that any retained information is stripped of personally identifying data. If there is potential for a Consumer Access Service to be sued for giving unauthorized access to a PHR, the Consumer Access Service should render the information

inaccessible to others but maintain an internal copy of identifiable information for defense purposes.

Area 6: Termination of Account

Just as the initiation of a PHR account must be voluntary, so must the termination of an account be a viable consumer choice.

Recommended Practice:

A Consumer Access Service must provide an easy-to-use mechanism for its users to terminate an account. Upon request of the consumer for account termination, the Consumer Access Service shall carry out such action without delay and within a reasonable timeframe.

Such mechanism should:

- Clearly state the consequences and actual definition of account termination.
- Provide a timely notice of the status of the request and any necessary follow-up communication to keep the consumer aware until such termination is complete.
- Provide, prior to account termination, an easy-to-use option for the consumer to export information to a personal computer or other Consumer Access Service. *(See **CT5: Portability of Information**.)*
- Provide the consumer with an option to expunge information.

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.*