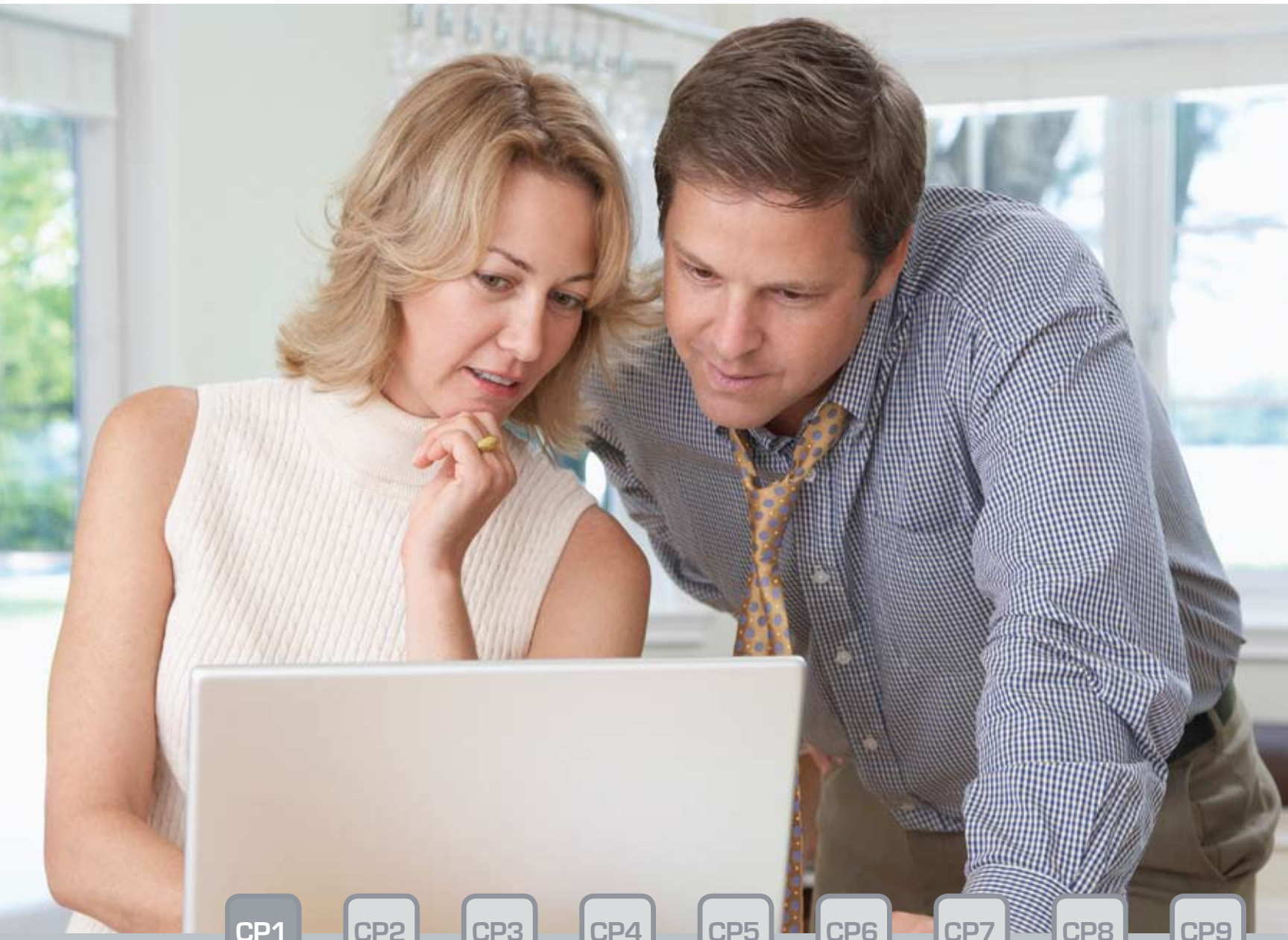


CP1 CP2 CP3 CP4 CP5 CP6 CP7 CP8 CP9

CT1 CT2 CT3 CT4 CT5 CT6 CT7

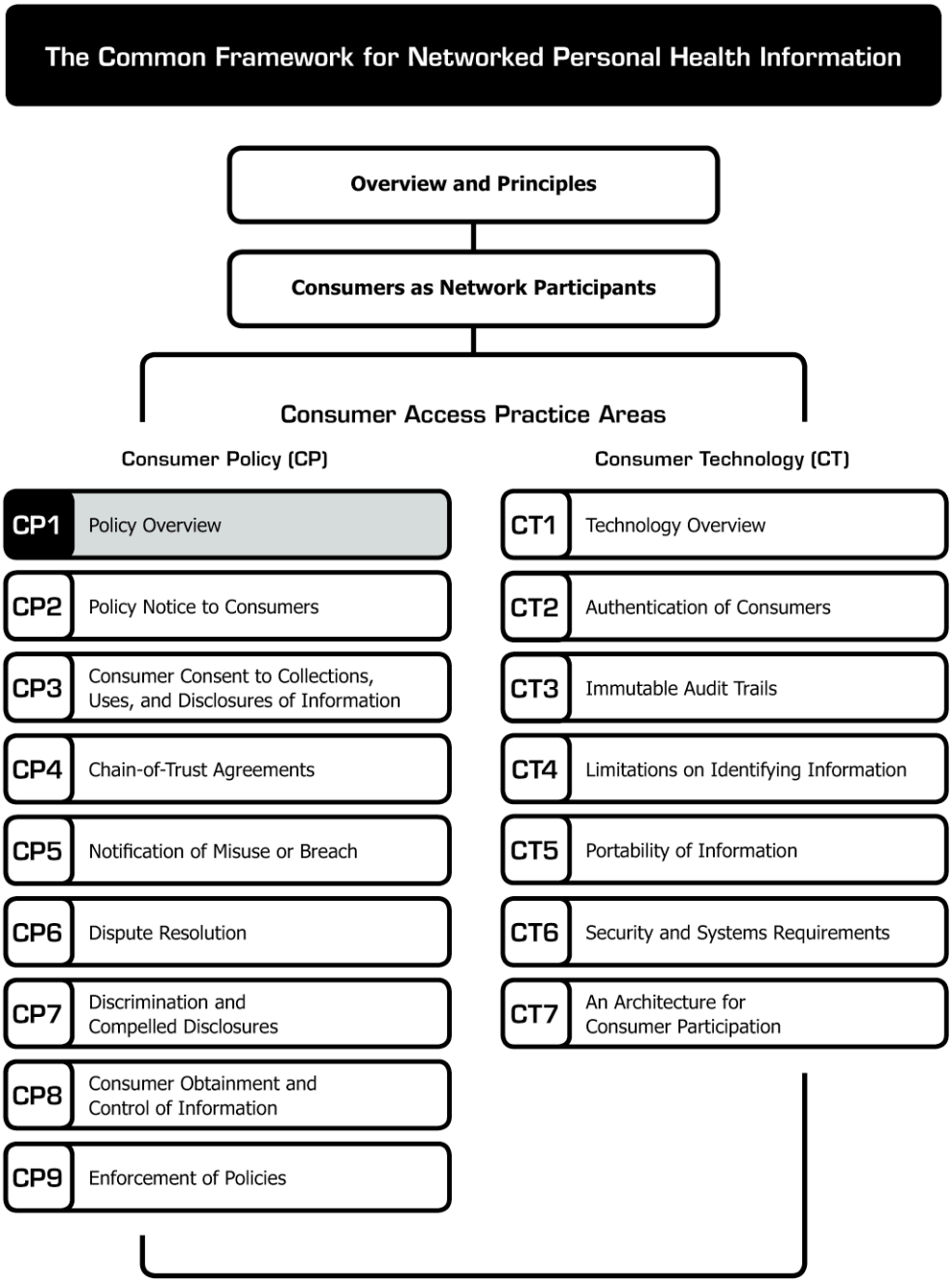
Policy Overview

Policy Overview

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:



Policy Overview*

Network services for personal health records (PHRs) are emerging in a complex and often uncertain legal and policy environment. In this paper, we discuss the policy landscape in the context of emerging Consumer Access Services — those services or organizations seeking to help individuals make electronic connections across multiple sources of their health information.

The Federal Regulatory Environment

Regulations promulgated under the Health Insurance Portability and Accountability Act (HIPAA), in effect since April 2003, put in place a set of privacy and security rules intended to build safeguards into the practice of health care. The Privacy Rule became law as public concern about the confidentiality of personal health information reached a high level, coupled with a growing awareness that the lack of privacy safeguards in health care heightened the risk that some people would choose to withdraw from full participation in their own care.

Under current federal statute[1] and regulation[2], there are three categories of Covered Entities that must comply with the HIPAA Privacy Rule: health care providers that transmit protected health information in electronic form to pay claims or engage in other standard transactions under the law, health plans, and health care clearinghouses.[3] In this respect, many of today's personal health record vendors do not qualify as Covered Entities and are not subject to the Privacy Rule.

The Privacy Rule includes:

- Requirements that Covered Entities provide notice to consumers of their rights and protections.
- Requirements that Covered Entities provide consumers with copies of or access to their information if requested.[4]
- Permissions for providers to use and disclose patient data, without consent, for treatment, payment, and health care operations (a broad category known as "TPO").
- Limitations on certain other uses and disclosures of identifiable patient information.
- Requirements for providers and other Covered Entities to obtain patient authorization for disclosures not expressly permitted by the Privacy Rule.
- Specific rules that permit disclosure under detailed conditions to researchers, law enforcement, and public health officials without the consumer's consent or authorization.
- Oversight and enforcement mechanisms.

* **Connecting for Health** thanks Josh Lemieux, Markle Foundation, and Janlori Goldman, JD, Health Privacy Project and Columbia University School of Public Health, for drafting this paper. A special thanks to Joy Pritts, JD, Center on Medical Record Rights and Privacy, Health Policy Institute, Georgetown University, for providing additional insights and reviews in developing this document.

©2008, Markle Foundation
This work was originally published as part of a compendium called *The **Connecting for Health** Common Framework for Networked Personal Health Information* and is made available subject to the terms of a license (License) which may be viewed in its entirety at: http://www.connectingforhealth.org/license.html. You may make copies of this work; however, by copying or exercising any other rights to the work, you accept and agree to be bound by the terms of the License. All copies of this work must reproduce this copyright information and notice.

1 42 U.S.C. 1302(a), 42 U.S.C. 1320d -1320d-8, and sec. 264 of Pub. L. 104-191, 110 Stat. 2033-2034 (42 U.S.C. 1320d-2(*note*)) and 5 U.S.C. 552.

2 Unofficial Version of HIPAA *Administrative Simplification Regulation Text*, 45 CFR Parts 160, 162, and 164, as amended through February 16, 2006, available at: http://www.hhs.gov/ocr/AdminSimpRegText.pdf.

3 45 CFR § 164.103.

4 **Connecting for Health** summarized HIPAA regulations related to consumer access in the Common Framework document *Patient's Access to Their Own Health Information.* Available online at: http://www.connectingforhealth.org/commonframework/docs/P6_Patients_Access.pdf.

Through its Office for Civil Rights[5], the U.S. Department of Health and Human Services (HHS) enforces the Privacy Rule directly as applied to Covered Entities. The Department of Justice is empowered to investigate and prosecute criminal violations of the law, and state enforcement mechanisms are also empowered to oversee and apply the law. According to the HHS Office for Civil Rights, since the Privacy Rule went into effect in April 2003, more than 29,000 voluntary complaints have been received, about 80 percent of which have been resolved. As of July 31, 2007, corrective action has been taken in fewer than 5,000 cases, most of which have been in the past 2 years.[6] There have been no civil penalties assessed and only a handful of criminal prosecutions under the Privacy Rule.

Related to the enforcement challenge are difficulties in interpretation of the Privacy Rule. Although it has been in place since 2003, many Covered Entities remain confused about what the Privacy Rule does and does not allow, as documented most recently by the Health Information Privacy and Security Collaborative (HISPC).[7]

Questions About the Current Policy Framework

Below are important questions on whether consumer protections and policy enforcement are adequate in the emerging environment of consumer data streams and networked PHRs.

Question 1: Does the HIPAA Privacy Rule apply to emerging Consumer Access Services?

Answer: Not necessarily. It depends on whether the Consumer Access Service is operated by, or on behalf of, a Covered Entity.

The Privacy Rule is limited by the scope of the HIPAA statute. Most notably, HIPAA only applies directly to Covered Entities — which many Consumer Access Services and PHRs are not. To the extent that a Covered Entity does offer a PHR directly to its patients or members, the Covered Entity must comply with the Privacy Rule. If the Covered Entity contracts with a third party to provide a PHR to consumers on its behalf, it must enter into a "Business Associate Agreement," which limits that contractor's use and disclosure of health information. These downstream entities are restricted in their use and disclosure only through contract law. In general, Business Associates are not directly regulated under HIPAA. As a result, if a Business Associate violates the contract, the Covered Entity can take the Business Associate to court under contract law. But it is the Covered Entity — not the Business Associate — that may be subject to regulatory enforcement action for the violation. (The regulation states that the Covered Entity is only liable when it knew of a Business Associate's breaches and took no action.)

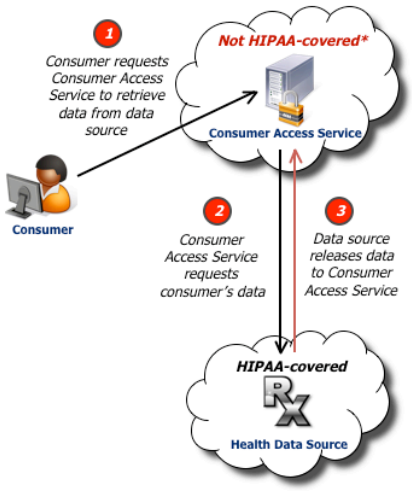
Thus, if a Covered Entity provides a Consumer Access Service to its patients, members, or employees, then the Covered Entity must comply with Privacy Rule requirements (even if the actual service is supplied by a vendor under a Business Associate agreement). However, if the Consumer Access Service is neither a Covered Entity nor acting as a Business Associate of a Covered Entity, it is not governed by the federal regulation. Such a Consumer Access Service may receive identifiable patient health data *that originated at a Covered Entity*[8] primarily in two ways:
A) From a Covered Entity based on an authorization from the consumer:

[5] The OCR web page has several resources related to HIPAA. See http://www.hhs.gov/ocr/hipaa/.

[6] OCR: *HIPAA Compliance and Enforcement; Numbers at a Glance*. Accessed online on August 24, 2007, at the following URL: http://www.hhs.gov/ocr/privacy/enforcement/numbersglance.html.

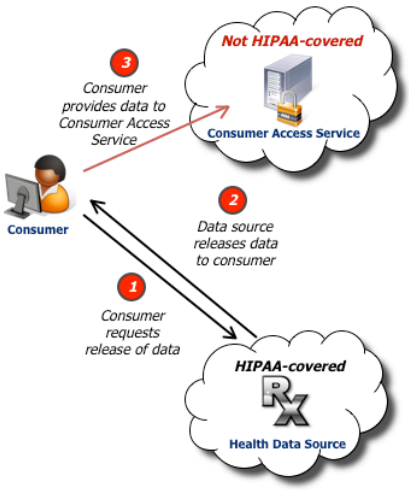
[7] Linda L. Dimitropoulos, RTI International, *Privacy and Security Solutions for Interoperable Health Information Exchange, Assessment of Variation and Analysis of Solutions Executive Summary and Nationwide Summary*. June, 20, 2007. Accessed online on August 24, 2007, at the following URL: http://www.rti.org/pubs/avas_execsumm.pdf. See also: http://www.rti.org/pubs/nationwide_execsumm.pdf.

[8] We emphasize that the diagrams depict possible flows of information "that originated at a Covered Entity" to a Consumer Access Service or PHR. The diagrams do not depict information that consumers may contribute themselves (e.g., patient diaries, self-populated problem lists, monitoring device data, etc.).



** Health Data Source may require a Business Associate Agreement under HIPAA.*

B) From the consumer who has obtained copies of her medical records directly from the Covered Entity and supplied them separately to the Consumer Access Service:



Some emerging Consumer Access Services are structured to encourage consumers to authorize their providers and plans to disclose health information directly to the Consumer Access Service. The public may not be aware that once the Consumer Access Service has received information from a Covered Entity based on the consumer's signed authorization, that information is no longer covered under the federal Privacy Rule. In other words, HIPAA privacy protections do not "follow" the data; they only apply when in the hands of a Covered Entity or its Business Associate(s). Non-covered organizations are not required to do many activities that are required of HIPAA-Covered Entities. For example, they are not required to train their staffs about privacy and confidentiality, or maintain an accounting of disclosures, or require an authorization before re-disclosing health information to other non-covered entities.

However, it is important to note that any organization in this marketplace — whether HIPAA-covered or not — can exceed the Privacy Rule requirements. Organizations may provide for higher levels of individual control over data flowing in or out of PHRs than are afforded to consumers under the Privacy Rule.

The HIPAA Privacy Rule did contemplate the use of networked health information systems, but only within the constraints of the Covered Entity/Business Associate framework. It is important to note that the HIPAA statute devoted little attention to e-health and privacy, let alone Consumer Access Services or networked PHRs.[9]

All new PHRs and Consumer Access Services demand thoughtful and carefully crafted practices to balance the need for consumer data streams to flow more readily with the need to protect privacy. A comprehensive approach to privacy is warranted in light of the emerging environment.

*(See the **Overview** document for Nine Core Principles for addressing privacy in a networked environment.)*

[9] See Mark Rothstein 2007 testimony to the National Committee on Vital Health Statistics and Congress. Accessed online on September 6, 2007, at the following URLs: http://www.hhs.gov/healthit/ahic/materials/06_07/cps/ncvhs.pdf. http://hsgac.senate.gov/_files/testimonyrothstien.pdf.

Question 2: How do HIPAA "treatment, payment, and operations" (TPO) rules apply when Covered Entities act as Consumer Access Services or offer PHRs?

Answer: To answer this question, consider the case of a person named Millie:

First, imagine that Millie goes to the doctor and receives a notice saying that her information can be used in various ways allowed under HIPAA. A year later, she visits the doctor's office and gets a treatment, and the doctor sends a claim to Millie's health insurance company. The insurance company then processes and pays the claim. The event generates several transactions and copies of information about Millie - none of which require Millie's specific consent. This is because under HIPAA, Covered Entities may make certain disclosures of personal health information for purposes of treatment, payment, and health care operations (TPO) without any consent from the consumer.[10]

Then, imagine that the insurance company offers Millie an online PHR that lets her view copies of that claims history. The mere fact that Millie is given an online account to view copies of claims does not change the nature of the health plan's permissible uses of the information under TPO rules.[11]

Now, let's imagine that the PHR offers Millie a chance to add her own contributions of information. For example, she could fill out a patient diary, or a health risk assessment, or perhaps enter a past diagnosis of which the health plan had previously been unaware. Or maybe Millie can connect her health plan PHR account to another source of health information about her, such as a home monitoring device or even from her other doctors or pharmacies. Do these new streams of information about Millie, captured through a PHR from a Covered Entity, fall under the TPO rules? Can they be used or disclosed the same way the claim from her doctor's office might be?

Clearly, such issues about HIPAA and TPO are clearly beyond the understanding of the average consumer. A more relevant question, therefore, is whether people like Millie can make informed choices about new personal health information services. Whether covered by HIPAA or not, organizations that offer Consumer Access Services or PHRs must have sound and transparent practices for consumer notice and consent, as well as the other areas of this framework. Sound practices for obtaining consumer consent include making choices proportional. That is, the more unexpected or disclosing the activity, the more specific the consent mechanism required to authorize it. *(See **CP2: Policy Notice to Consumers*** and ***CP3: Consumer Consent to Collections, Uses, and Disclosures of Information***.)

Question 3: Do state laws provide adequate protection of and support for consumer data streams?

Answer: Existing state health privacy laws are generally directed at health care providers and health plans. The vast majority are virtually silent on emerging developments such as regional health information exchanges or networked PHRs.[12] The result is that state law may restrict the circumstances under which a Health Data Source may send data to a PHR (such as by requiring patient consent), but does not protect the information once it has been transferred to the PHR.

Furthermore, to the extent that state laws may protect health information in consumer data streams, they often do so inconsistently. HIPAA sets a floor of protections, and does not

[10] For definitions of "treatment, payment, and operations," see: *Uses and Disclosures For Treatment, Payment, And Health Care Operations [45 CFR 164.506].* Accessed online on April 10, 2008, at the following URL: http://www.hhs.gov/ocr/hipaa/guidelines/sharingfortpo.pdf.

[11] Some plans may choose to segregate copies of information they provide to consumers through PHRs from the copies of information they use for their TPO-related uses. Other plans may not support this concept of a firewall between their TPO operations and their PHR operations.

[12] A notable exception is California law which treats a corporation organized for the purpose of maintaining medical information in order to make the information available to the patient or to a provider of health care at the request of the patient or a provider of health care, for purposes of diagnosis or treatment of the patient, as a provider of health care subject to the requirements of the state's Confidentiality of Medical Information Act. *See* Cal. Civ. Code § 56.06.

displace state laws that are more stringently privacy-protective. Many states have more stringent safeguards in place to impose condition- or issue-specific safeguards (i.e., HIV/AIDS, mental health, genetic information), or to address consumer access to their own records (e.g., requiring health care entities to respond more rapidly to consumer requests for records than HIPAA requires). These state laws may impose differing standards on different Health Data Sources and impact their ability to transfer health information to a PHR.

The National Council of State Legislatures (NCSL) and the National Governor's Association have launched an initiative to explore the need for new and consistent policies. Efforts are also underway at the federal level (in the Health Information Privacy and Security Collaboration and in legislative proposals) to "harmonize" state health privacy laws to avoid variations that some believe impede interoperability and data sharing. However, a number of studies suggest that most variations in state law can be addressed through policy and technical solutions.[13]

Overall, however, the lack of federal and state regulation, as well as the evolving interplay of state and federal laws, results in an uncertain regulatory environment. This can be chilling to the nascent market of Consumer Access Services. Fundamental questions about consumer consent for uses and disclosures, notice, enforcement, and chain-of-trust agreements are being determined outside of the regulatory environment, and many companies are uncertain how to proceed in their early products and services.

Question 4: Will business practices evolve to enhance consumer data streams and foster consumer trust?

Answer: Perhaps, but certainly not yet — and not consistently across the industry.

There is some hope that vendors' recognition of public concern about safeguarding personal information will drive competition to produce services with stronger and more responsive privacy components. Today, in the absence of regulatory clarity, most PHR ventures develop and adopt their own privacy and security policies, either as individual companies, or through trade and professional associations. However, such policies are inconsistent and often confusing. Because consumers do not have simple or foolproof ways to distinguish good privacy practices from bad, organizations may not be motivated to compete on the basis of privacy protection, and/or determine that "mining" personal data is more profitable than investing in stronger privacy protections. It is not clear there is a "market" for privacy, since many of the practices that would assure privacy safeguards are not observable by consumers. *(The potential role of regulation of PHRs and Consumer Access Services by the Federal Trade Commission (FTC) is discussed in* ***CP9: Enforcement of Policies****.)*

[13] For a survey of state privacy laws, see Georgetown University, *The State of Health Privacy, Second Edition, A Survey of State Health Privacy Statutes*, June 2002. Accessed online on August 24, 2007, at the following URL: http://hpi.georgetown.edu/privacy/pdfs/statereport1.pdf. See also the report issued in 2007 by the George Washington University that concludes that much of these state laws do not act as a barrier to health information exchange and interoperability. Reproduced with permission from BNA's Health Care Policy Report, Vol. 15, No. 11, 03/19/2007. Copyright

Question 5: Is there a need for a Common Framework of practices for Consumer Access Services and networked PHRs?

Answer: Yes, for the following reasons:

1. **The status quo poses increased risk:** If Consumer Access Services are successful in aggregating information from multiple sources, this creates both potential benefit and potential risk of exposure for the individual.
2. **The status quo lacks regulatory clarity:** The characteristics of the emerging PHR market suggest that at least some services will remain wholly or in part beyond the auspices of HIPAA. There is no consensus for how policies will be enforced in such situations.
3. **The status quo confuses consumers about privacy protections:** Faced with myriad PHR offerings and handlers of their electronic health data, consumers cannot be expected to be able to discern whether or not a particular data flow is covered by HIPAA or state law. In the absence of consistent privacy assurances that apply to all Consumer Access Services across the nation, many consumers will be making choices in an uncertain policy landscape.
4. **The status quo keeps 'notice' and 'consent' moving targets:** Recent surveys of PHRs indicate wide variance in privacy policies and forthrightness about critical issues such as how information will be used.[14] Notices to consumers are typically lengthy, in fine print, with language that may be simultaneously technical and vague. Policies are non-standardized and often disorganized, with multiple notifications about how personal data are collected, stored, protected, used, and disclosed. Without consistent policies, this wide variance of privacy and security practice disclosure is likely to continue, leading to a confusing marketplace.
5. **Common practices will aid trust on a network:** Certainly, there must be a clear need for private entities to share data on the consumer's behalf. However, a truly open and innovative market that can meet consumer needs is unlikely to flourish without a set of common practices that manage risk acceptably for Consumers, Health Data Sources, and Consumer Access Services.

[14] Altarum, *Review of the Personal Health Record (PHR) Service Provider Market: Privacy and Security*. March 13, 2007. Available at: http://www.hhs.gov/healthit/ahic/materials/03_07/ce/report.doc. See also ***CP2: Policy Notice to Consumers***.

Public Concern about Privacy

Frequent news reports remind Americans about the risks to their health privacy by theft, breach, and unauthorized or unwelcome disclosure of their personal health information.[i] Eight in 10 Americans say they are "very concerned" about the risk of identity theft and fraud with networked personal health records, according to a Markle Foundation 2006 survey.[ii] Concerns are intensified in the context of electronic information sharing, as documented by a 2007 survey showing that the public believes a computer-based medical records system is less secure than a paper-based one.[iii] Three in five Americans believe that their health information is not adequately protected under federal and state laws and current business practices, according to a Harris Interactive study commissioned by the Institute of Medicine.[iv]

Moreover, such concerns can lead to privacy protective behaviors that actually undermine health, particularly among members of the most vulnerable demographic groups. Surveys consistently show that people with chronic diseases and racial and ethnic minorities are the most likely to withhold information from providers and avoid care to shield themselves from discrimination, stigma, and unwanted exposure.[v]

[i] A collection of abstracts of news reports addressing health privacy events is available on the web site of Health Privacy Project at: http://www.healthprivacy.org/usr_doc/Privacystories.pdf.

[ii] Markle Foundation December 7, 2006 press announcement, *Survey Finds Americans Want Electronic Personal Health Information to Improve Own Health Care*. Available at: http://www.markle.org/downloadable_assets/research_doc_120706.pdf.

[iii] See Health Care Information Technology Summit Survey Results by Kaiser Permanente. May 2, 2007. Available at: http://xnet.kp.org/newscenter/kphealthconnect/healthitsurvey.html.

[iv] Government Health IT, *Surveys Show Public Distrusts HIPAA; Researchers Detest It*. Accessed online on October 3, 2007, at the following URL: http://www.govhealthit.com/online/news/350058-1.html.

[v] See Ann Bagchi, Lorenzo Moreno, and Raquel af Ursin, *Considerations in Designing Personal Health Records for Underserved Populations*. April, 2007. Available at: http://www.mathematica-mpr.com/publications/pdfs/hlthcaredisparib1.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.*