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

CT1 CT2 CT3 CT4 CT5 CT6 CT7

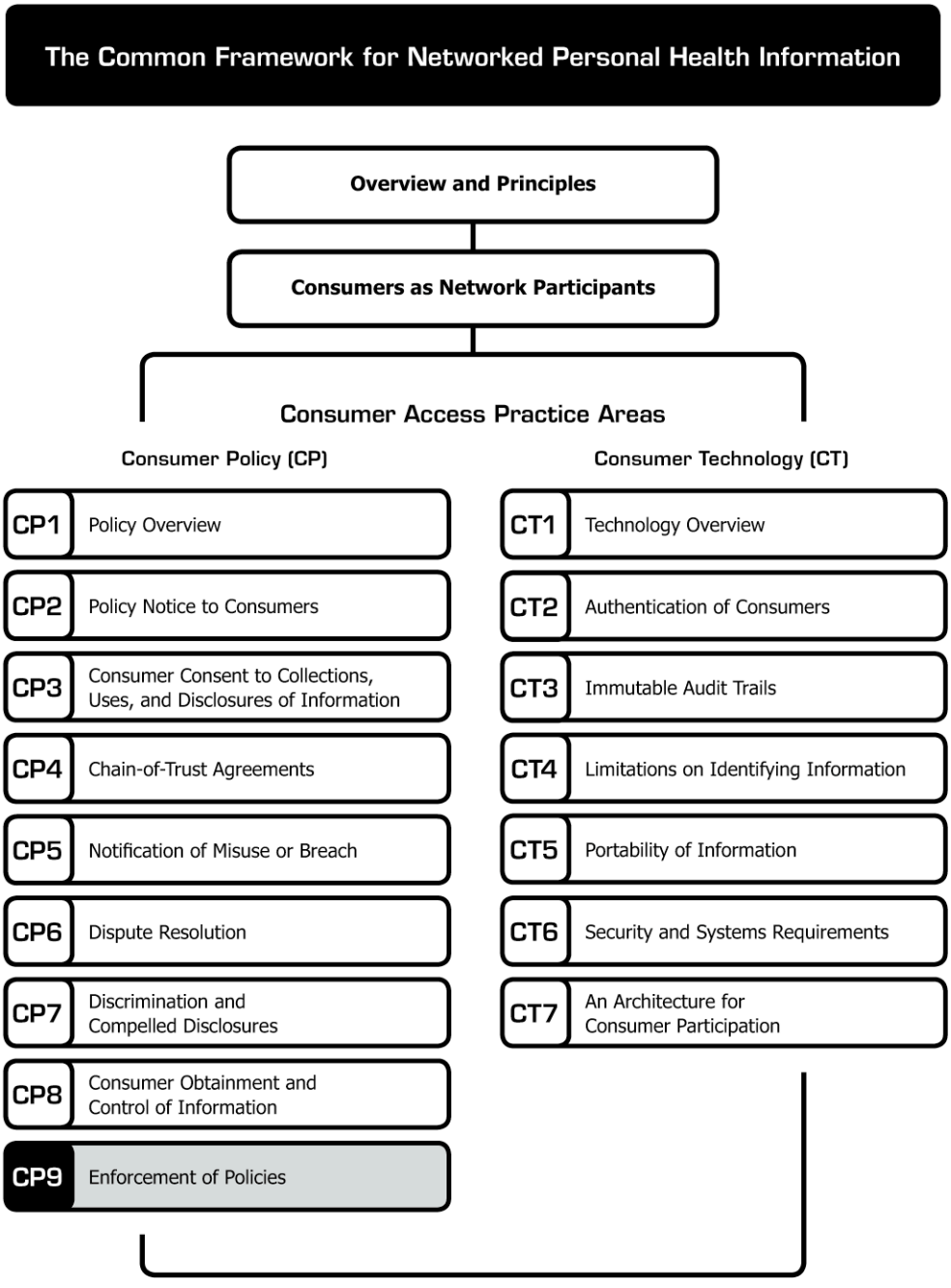
Enforcement of Policies

Enforcement of Policies

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:



Enforcement of Policies*

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

8. Accountability and oversight

9. Remedies

* "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.

All participants in health information networks must confront the question of how policies and practices will be enforced. Many consumers and decision-makers in the business community are likely to perceive an unregulated environment for Consumer Access Services and networked PHRs to be risky and unsafe for the long term. Further, policies and practices that vary widely between entities will be confusing. *(See **CP1: Policy Overview**.)* It is important, moreover, to encourage competition and innovation that leads to higher levels of privacy and security protections for consumers.

In the absence of new federal law, rules are needed to bind Consumer Access Services and PHR suppliers to a set of agreed-upon policies and practices. The discussion should consider a full range of possible enforcement options. The advantages and disadvantages of additional enforcement mechanisms should be robustly debated to determine what additional means are optimal, which may vary depending on the type of policy to be enforced.

Among the mechanisms to consider:

Future Enforcement Option 1: Strengthen Oversight and Enforcement of Current Law

- **Potential advantages:** Existing laws (mainly the HIPAA Privacy Rule and FTC authority) provide a range of mechanisms for federal regulators to enforce current privacy protections. The Office for Civil Rights (OCR) at the Department of Health and Human Services (HHS) has authority to investigate complaints under the Privacy Rule and to impose civil penalties. The U.S. Department of Justice (DOJ) is empowered to investigate potential criminal violations of the Privacy Rule and to seek criminal penalties where appropriate. Further, the Federal Trade Commission (FTC) has the authority to investigate violations of privacy under its general authority to punish "unfair and deceptive" trade practices; the FTC uses this authority, for example, against entities that violate their published privacy policies. HHS could improve enforcement and even have an impact on entities and services not covered by HIPAA by issuing guidance on key issues. For example, HHS could develop a model privacy notice, just as it has issued a model Business Associates agreement. *(See **CP1: Policy Overview**.)*
- **Potential disadvantages:** Enforcement of the HIPAA Privacy Rule has not been robust. OCR has received nearly 30,000 voluntary complaints alleging violations of the Privacy Rule, but has not yet imposed a civil penalty. In a few cases, the DOJ has brought criminal charges, mainly where medical records were used for financial fraud, identity theft, or to reveal an individual's identity. Moreover, HIPAA does not cover many Consumer Access Services and PHRs. The FTC is just beginning to assess its role in enforcing privacy for health information services on the

* **Connecting for Health** thanks Josh Lemieux, Markle Foundation, for drafting this paper. A special thanks to Jim Dempsey, JD, Center for Democracy and Technology, for contributions and insights in this paper.

Internet.[1] Nor has this emerging market adopted comprehensive, agreed-upon privacy notices. Gaps and uncertainties in current law make its enforcement in this regard mostly inapplicable to many Consumer Access Services.

Future Enforcement Option 2: Amend HIPAA to Extend the Privacy Rule to Cover Consumer Access Services and PHRs That Are Not Currently HIPAA-Covered

- **Potential advantages:** Some suggest that amending existing law may be an effective mechanism for achieving national standards that support the development of Consumer Access Services with privacy and security safeguards in place. A wide variety of constituents and perspectives can be considered in a federal forum (hearings, reports, public comment) that may result in either a significant consensus, or a set of minimum standards from which to begin.
- **Potential disadvantages:** There is a widespread lack of enthusiasm and outright resistance to "re-opening" HIPAA, some of which may be rooted in a desire to avoid new regulation, but which also seems to be a side effect of what some consider to be a history of divisiveness, confusion, and misinterpretation experienced in its creation and implementation (most recently documented by HISPC[2]). To date, the capacity of the HHS Office for Civil Rights has not been adequate to meet the demand for guidance and enforcement. Amending HIPAA to cover Consumer Access Services may re-ignite old disagreements regarding the statutory constraints of HIPAA and may stifle rather than encourage the development of Consumer Access Services.

*(See **CP1: Policy Overview** for further discussion on the HIPAA Privacy Rule and emerging Consumer Access Services and PHRs.)*

Future Enforcement Option 3: Enact Separate Federal Laws Specifically to Govern Consumer Access Services

- **Potential advantages:** Enacting separate laws for Consumer Access Services and PHRs may avoid the challenges involved in amending HIPAA and may provide an opportunity for a fresher, more contemporary approach to regulating emerging health information products, services, and entities.
- **Potential disadvantages:** New laws, separate from HIPAA, may be interpreted as "re-inventing the wheel," instead of building on the policies and practice framework already promulgated in the HIPAA Privacy and Security Rules.

Future Enforcement Option 4: Strengthen and Modernize State Laws to More Clearly Address Privacy

- **Potential advantages:** States can be leaders in the innovation of privacy protections. State laws could be updated to apply to changes in the health care and information environments. A hybrid model, which has been considered in other sectors, would give state Attorneys General the authority to enforce federal rules, thereby drawing on the resources of those offices.
- **Potential disadvantages:** Enacting new laws that vary from state to state will contribute to the uneven patchwork of protections that exist today. Given that Consumer Access Services, PHRs, and other health information-sharing efforts are not always geographically defined, a geographically based regulatory approach may prove to be impractical, expensive, and confusing in a networked environment.

---

[1] On April 24, 2008, the FTC held a workshop on this subject. Presentations accessed online on May 8, 2008, at the following URL: http://www.ftc.gov/bc/healthcare/hcd/index.shtm.

[2] 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.

Future Enforcement Option 5: Leverage the Buying Power of Government and Employers by Requiring Adherence to Certain Policies as a Condition for Procurement

- **Potential advantages:** Health care "purchasers" include the federal government and states with Medicare and Medicaid programs for citizens and health benefits packages for public employees, as well as employers that contract for provider and payer services on behalf of employees. Medicare and Medicaid alone account for more than one-third all of health care expenses.[3] It could potentially have a significant accelerating impact if government programs and employer coalitions required that their contractors adhere to certain practices to improve the consumer's ability to obtain electronic copies of their information, as well as to protect personal information from misuse or abuse. Of course, the government has several tools to ensure compliance with its contracts, ranging from withholding business or payment to regulatory action or even criminal prosecution (presumably in egregious cases).
- **Potential disadvantages:** It is difficult for large federal agencies and employer coalitions to define the optimal level of requirements to achieve intended consequences and avoid adverse unintended consequences. For example, requirements could be too heavy-handed or too rigid, perhaps locking in certain contractors or technologies and thereby stifling competition or innovation.

Future Enforcement Option 6: Encourage Self-Attestation with Third Party Validation

- **Potential advantages:** Consumer Access Services could adopt an industry standard requiring that they be audited by independent organizations. Participating Consumer Access Services would publish statements indicating their conformance to industry standards and would subject themselves to independent validation of their claims. Such validation could be performed by independent entities, which could also inspect the compliance of the Consumer Access Service's business partners. Such a requirement could signal greater transparency in the industry, with greater accountability and controls. Other models of certification or accreditation may be relevant.
- **Potential disadvantages:** Until there are industry standards upon which to validate Consumer Access Services, this option is not practical. Even if standards were available, however, this option poses additional challenges. First, it is difficult to structure validation entities to be truly independent of the entities they examine. Second, validation and certification are most successful when specific technical requirements can be specified through an industry-accepted process, then tested separately via trusted and independent bodies. Third, privacy practices usually reflect the behavior of organizations and individuals, and thus cannot be prospectively tested. Fourth, certification is inherently conservative, reflecting current industry capabilities. In a new area such as Consumer Access Services, where best practices have not been validated, it is important to encourage innovative ways to achieve privacy and individual control, rather than bind the industry to current, largely inadequate, options.

[3] NHE Fact Sheet, Centers for Medicare & Medicaid Services. 2006. Accessed online on April 11, 2008, at the following URL: http://www.cms.hhs.gov/NationalHealthExpendData/25_NHE_Fact_Sheet.asp#TopOfPage.

Future Enforcement Option 7: **Encourage Consumer-Based Ratings and Online Community-Based Self-Policing**

- **Potential advantages:** "Web 2.0" applications increasingly rely on consumers to rate services (e.g., hotels, restaurants), products (e.g., movies, books, cars, appliances), and people (e.g., blog posts, eBay transactions), etc. Such "community policing" is extremely efficient, given that the content is generated for free by consumers. Composite data from consumer surveys can be especially helpful when combined with independent testing, as is done, for example, by Consumer's Union or PC Magazine.
- **Potential disadvantages:** Online forums can devolve into polarizing discussions. They also can take a while to build a critical mass of data that is useful for comparing various services. More importantly, many consumers are simply not in a position to rate the data-handling practices of Consumer Access Services, since many critical backend activities are not observable.

Conclusions

It is clear that there will not be one single mechanism that optimally and comprehensively enforces the full complement of practices in a Common Framework for Networked Personal Health Information. Instead, it is likely that enforcement will best be achieved by a mix of strategies, tailored to the specific practices identified in the proposed framework. Even achieving enforcement of any given practice may require a mix of approaches. It is also likely that effective enforcement will have to evolve over time. Because we expect Consumer Access Services to develop incrementally, it is difficult to imagine a "big bang" approach to enforcement that will be able to encompass the complexity of the market and the ongoing changes in business models for Consumer Access Services. The states may experiment with various approaches, while federal policymakers may take an incremental approach, addressing some issues before others. Finally, it is clear that participants in the policymaking process should keep in mind the full Common Framework, and not overemphasize one practice to the exclusion of the others, for they are intended to function, over time, as an inter-related whole.

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.*