CP1 CP2 CP3 CP4 CP5 CP6 CP7 CP8 CP9

CT1 CT2 CT3 CT4 CT5 CT6 CT7

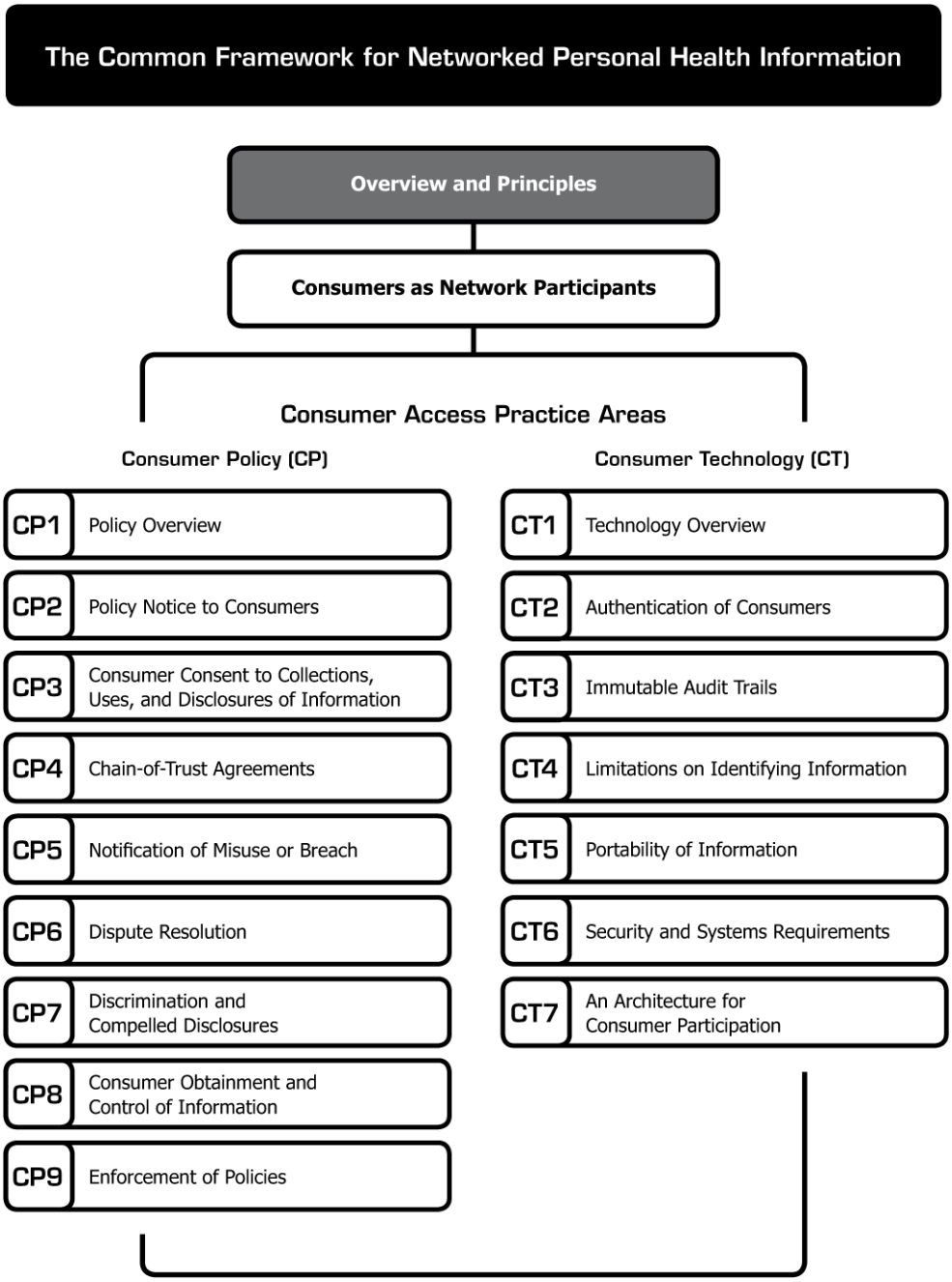
Overview and Principles

Overview and Principles

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:



Overview and Principles*

Many policy and industry leaders now agree that empowerment of consumers — enhanced by convenient access to networked health information services — will help drive necessary changes to the health care sector. The **Connecting for Health** Common Framework for Networked Personal Health Information provides a foundation for maintaining trust among all participants — business, professional, and consumer — in electronic health information networks.

The objective is to give consumers the ability to compile electronic copies of their personal health information, including their own contributions, under a set of fair practices that respect personal preferences for how information may be collected and shared. The term "networked" implies connectivity across entities. Networking health information is critical given the fragmentation of most health-related services in the United States.

Connecting for Health — a public-private collaborative group engaging more than 100 organizations representing all major components of the health sector — convened the Work Group on Consumer Access Policies[1] to identify a set of practices to support the emergence of networked personal health records (PHRs) in the public interest. PHRs include a wide variety of electronic applications designed to help consumers manage their health-related information and transactions, communicate better with clinicians, or take better care of themselves and loved ones.

The Common Framework resources are intended to foster network relationships and, ultimately, to enhance trust among the following parties:

- **Consumers**, including patients, their families, and caregivers. Our vision is that individual consumers will be able to compile and share electronic copies of their personal health information captured at various points, including the home (e.g., monitoring devices, patient diaries).
- **Heath Data Sources**, meaning any institutional custodian of the individual's personal health information. This may include health care providers and clinics, hospitals and health care systems, health insurance plans, clearinghouses, pharmacies and pharmacy benefit managers, laboratory networks, disease management companies, and others that hold data related to the personal health of individuals.
- **Consumer Access Services**, an emerging set of services designed to help individuals make secure connections with Health Data Sources in an electronic environment. Consumers may be offered such services by a variety of organizations, ranging from existing health care entities (e.g., providers, payers, self-insured employers) to new entrants to the

* This framework is the product of the **Connecting for Health** Work Group on Consumer Access Policies for Networked Personal Health Information. *(See Work Group roster in **Acknowledgements**.)* **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 guiding the documents. We particularly thank Carol Diamond, MD, MPH, Managing Director of the Health Program at the Markle Foundation, for developing the conceptual structure for this approach to networked personal health information.

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.

[1] See **Acknowledgments** for a roster of the **Connecting for Health** Work Group on Consumer Access Policies.

health sector (e.g., technology companies, employer coalitions, affinity groups, health record banks, etc.). Such services are likely to provide functions such as authentication as well as data hosting and management.

We distinguish Consumer Access Services from PHR applications (although both could be supplied in one integrated product). Consumers ideally will have a choice of services to enable PHR applications of their choosing to exchange data with multiple Health Data Sources across a secure "network of networks."[2] The diagram above illustrates this basic distinction.

The rationale for Consumer Access Services rests primarily on two points:

1. It is not practical for most individuals to connect separately and differently to every institution that holds their health data, and
2. In an open and innovative market, individuals should choose applications that best meet their own needs, rather than be solely reliant on the applications offered by the various institutional sources of their health information or services.

The Common Framework resources are designed to guide organizations participating in what we call "consumer data streams" — the flow of personal health information into and out of consumer-accessible applications such as PHRs. (*See* ***CT1: Technology Overview*** *for a discussion of "consumer data streams" and how they contrast with "business data streams*.")

There are many emerging consumer data streams today. Hundreds of PHR applications now offer a variety of services to U.S. consumers, including products sponsored by providers, health plans, employers, technology companies, non-profits, and others. Several global brands have launched initiatives to act as Consumer Access Services. There also is a growing number of patient community sites, often described as "Health 2.0," that take innovative approaches to health problems from outside traditional health care.

Public opinion surveys commissioned by the Markle Foundation[3] and others have found that most Americans want to have electronic copies of their health records. The research indicates that Americans understand that quality of care could improve when their health information is

[2] By analogy, a cell phone is an application, and a cellular service connects the application to a network of towers that allow the phone to connect with other cell phones. Similarly, the PHR is an application, and a Consumer Access Service provides network services enabling a consumer to receive and send information through a PHR application.

[3] 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: http://www.markle.org/downloadable_assets/research_doc_120706.pdf.

available over the Internet to them and those who care for them. Markle also found that eight in 10 Americans are very concerned about identity theft or fraud, and the possibility of their data being used by marketers without their permission.

This Common Framework provides a voluntary approach to meet the dual challenges of making personal health information more readily available to consumers, while also protecting it from unfair or harmful practices.

Connecting for Health Core Principles

Connecting for Health has published a set of principles that provide the foundation for managing personal health information within consumer-accessible data streams. The consensus principles — based on accepted international fair information practices — are presented fully in *The Architecture for Privacy in a Networked Health Information Environment*.[4] Taken together, the nine principles form a comprehensive approach to privacy, the hallmark for which is that personal information be handled according to the individual's understanding and consent. In brief, the principles, and the corresponding papers in this Framework, are as follows:

[4] Available online at: http://www.connectingforhealth.org/commonframework/p1.html.

Connecting for Health Core Principles	Practice Areas of this Common Framework for Networked Personal Health Information
1. **Openness and transparency:** Consumers should be able to know what information has been collected about them, the purpose of its use, who can access and use it, and where it resides. They should also be informed about how they may obtain access to information collected about them and how they may control who has access to it.	***CP2:*** *Policy Notice to Consumers*
2. **Purpose specification:** The purposes for which personal data are collected should be specified at the time of collection, and the subsequent use should be limited to those purposes, or others that are specified on each occasion of change of purpose.	***CP2:*** *Policy Notice to Consumers* ***CP3:*** *Consumer Consent to Collections, Uses, and Disclosures of Information* ***CT4:*** *Limitations on Identifying Information*
3. **Collection limitation and data minimization:** Personal health information should only be collected for specified purposes and should be obtained by lawful and fair means. The collection and storage of personal health data should be limited to that information necessary to carry out the specified purpose. Where possible, consumers should have the knowledge of or provide consent for collection of their personal health information.	***CP2:*** *Policy Notice to Consumers* ***CP3:*** *Consumer Consent to Collections, Uses, and Disclosures of Information* ***CT4:*** *Limitations on Identifying Information*
4. **Use limitation:** Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified.	***CP2:*** *Policy Notice to Consumers* ***CP3:*** *Consumer Consent to Collections, Uses, and Disclosures of Information* ***CP7:*** *Discrimination and Compelled Disclosures* ***CT3:*** *Immutable Audit Trails* ***CT4:*** *Limitations on Identifying Information*
5. **Individual participation and control:** Consumers should be able to control access to their personal information. They should know who is storing what information on them, and how that information is being used. They should also be able to review the way their information is being used or stored.	***CP3****: Consumer Consent to Collections, Uses, and Disclosures of Information* ***CP5:*** *Notification of Misuse or Breach* ***CP7:*** *Discrimination and Compelled Disclosures* ***CP8:*** *Consumer Obtainment and Control of Information* ***CT3:*** *Immutable Audit Trails* ***CT5:*** *Portability of Information*

6. **Data quality and integrity:** All personal data collected should be relevant to the purposes for which they are to be used and should be accurate, complete, and up-to-date.	***CP6:*** *Dispute Resolution* ***CP8:*** *Consumer Obtainment and Control of Information* ***CT2:*** *Authentication of Consumers* ***CT3:*** *Immutable Audit Trails*
7. **Security safeguards and controls:** Reasonable safeguards should protect personal data against such risks as loss or unauthorized access, use, destruction, modification, or disclosure.	***CP5****: Notification of Misuse or Breach* ***CT2:*** *Authentication of Consumers* ***CT4:*** *Limitations on Identifying Information* ***CT6:*** *Security and Systems Requirements* ***CT7:*** *An Architecture for Consumer Participation*
8. **Accountability and oversight:** Entities in control of personal health information must be held accountable for implementing these principles.	***CP4:*** *Chain-of-Trust Agreements* ***CP5:*** *Notification of Misuse or Breach* ***CP6:*** *Dispute Resolution* ***CP9:*** *Enforcement of Policies* ***CT3:*** *Immutable Audit Trails*
9. **Remedies:** Remedies must exist to address security breaches or privacy violations.	***CP5:*** *Notification of Misuse or Breach* ***CP6:*** *Dispute Resolution* ***CP9****: Enforcement of Policies*

The general standard is that practices must not be misleading or unfair. Misleading practices include misrepresentations or omissions that may contribute to a reasonable consumer's decision to use a service, provide personal data, or grant permissions relating to that data.[5] Unfairness may occur when consumers are injured after being forced or coerced into making decisions in the marketplace that are not their own.[6] Emerging consumer data streams must be based on trusted and transparent relationships, without behind-the-curtain uses or disclosures of personal information that would catch an average consumer unawares. It would be alarming for consumers, as well as all legitimate network participants, if consumer data streams were harnessed by "shadow" businesses that exploit indirect and involuntary relationships with consumers.

[5] See the Federal Trade Commission's *1983 Policy Statement on Deception*. Accessed online on August 28, 2007, at the following URL: http://www.ftc.gov/bcp/policystmt/ad-decept.htm.

[6] See the Federal Trade Commission's *1980 Policy Statement on Unfairness*. Accessed online on October 22, 2007, at the following URL: http://www.ftc.gov/bcp/policystmt/ad-unfair.htm.

Practice Areas for Networked Personal Health Information

We contend that a foundational set of practices, rooted in the above principles, would help sustain public confidence in consumer data streams. We sought to propose a set of practices that, when taken together, encourage appropriate handling of personal health information. The Consumer Framework for Networked Personal Health Information introduces nine policy and seven technical resources that provide a foundation for organizations doing any of the following:

1. Collecting, receiving, storing, or using personal health information as part of a consumer data stream or PHR services.
2. Transmitting or disclosing to a third party any personal health information gathered through or derived from a consumer data stream or PHR services.

At this early point in the evolution of PHRs and services to support them, we propose this as a voluntary framework. We recommend that all organizations develop clear and public policies for each of the practice areas in this framework. *All practice areas must be addressed to provide adequate protections to consumers and to encourage trust across a network*.

The framework consists of Consumer Policy (CP) and Consumer Technology (CT) papers, although there is often not a firm distinction between policy and technology. Indeed, it is a hallmark of the Common Framework approach that decisions on policy and technology are interdependent.

Consumers as Network Participants: Explains why consumer participation can be transformative in health care as it has been in other sectors; why networked PHRs are a vital tool to empowering consumers, and how policies can help guide an emerging industry.

CP1: Policy Overview: Describes the policy landscape, including how the Health Information Portability and Accountability Act (HIPAA) as well as state and contract laws apply to emerging consumer data streams. Explains unregulated and regulated areas of the current environment, and argues for a voluntary common framework of policies.

CP2: Policy Notice to Consumers: Recommends preferred practices for giving consumers access to the policies for collection, use, and disclosures of personal health information, including privacy and security practices, terms and conditions of use, and other relevant policies.

CP3: Consumer Consent to Collections, Uses, and Disclosures of Information: Describes mechanisms to capture the consumer's agreement prior to any collection, use, or disclosure of personal data; explains why notice and consent are not sufficient by themselves in providing adequate protection for consumers.

CP4: Chain-of-Trust Agreements: Describes the merits and limitations of contractual mechanisms among parties exchanging personal health information; recommends important limitations to place on unaffiliated third parties, including vendors, service providers, and others who receive personal data or de-identified data.

CP5: Notification of Misuse or Breach: Discusses what to do if something goes wrong. Recommends that consumers be individually informed if their personal information was, or is reasonably believed to have been, disclosed or acquired by an unauthorized person or party in a form that carries significant risk of compromising the security, confidentiality, or integrity of personal information.

CP6: Dispute Resolution: Recommends that consumers be provided a clear and logical pathway to resolve disputes such as over breach or misuse, data quality or matching errors, allegations of unfair or deceptive trade practices, etc.

CP7: Discrimination and Compelled Disclosures: Recommends policies to bar discrimination and "compelled disclosures" — such as when the consumer's authorization for release of data is required in order to obtain employment, benefits, or other services.

CP8: Consumer Obtainment and Control of Information: Covers several areas to facilitate the consumer's ability to electronically collect, store, and control copies of personal health information, including requesting data in an electronic format, allowing for proxy access to an account, requesting amendments, or disputing entries of data. Also covers appropriate retention of information in inactive accounts, and consumer requests to "delete" data and terminate their accounts.

CP9: Enforcement of Policies: Raises the issue of how policies and practices should be enforced on the network; describes the pros and cons of several different enforcement mechanisms, including: enforcing current laws, amending and expanding HIPAA, creating new law to govern Consumer Access Services, encouraging self-attestation with third-party validation, and encouraging consumer-based ratings.

CT1: Technology Overview: Describes the complexity of emerging digital health data streams; explains how information can be combined to build revealing profiles of individuals; depicts how health care entities and consumer technology innovators operate under different cultures that can clash without basic rules of the road.

CT2: Authentication of Consumers: Provides a framework for establishing and confirming the identity of individual consumers so that they may participate on a network.

CT3: Immutable Audit Trails: Recommends that audit trails be a basic requirement of PHRs and supporting services; explains the value of providing consumers with convenient electronic access to an audit trail as a mechanism to demonstrate compliance with use and disclosure authorization(s).

CT4: Limitations on Identifying Information: Recommends strong limitations on disclosures of identifying data to third parties. Supports disclosures only of those data that are reasonably necessary to perform the limited function(s) to which the third parties are authorized. Provides a caveat about considering data "de-identified."

CT5: Portability of Information: Highlights the importance of the consumer's ability to export and import information in industry-standard formats as they become available.

CT6: Security and Systems Requirements: Provides a brief outline on basic security protections. Recommends continuous monitoring of industry practices and threats, as well as personnel training and strict policies regarding who can access consumer data, and consequences for security violations.

CT7: An Architecture for Consumer Participation: Provides a view on how Consumer Access Services can fit within the **Connecting for Health** approach to architecture for a Nationwide Health Information Network (NHIN).

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.*

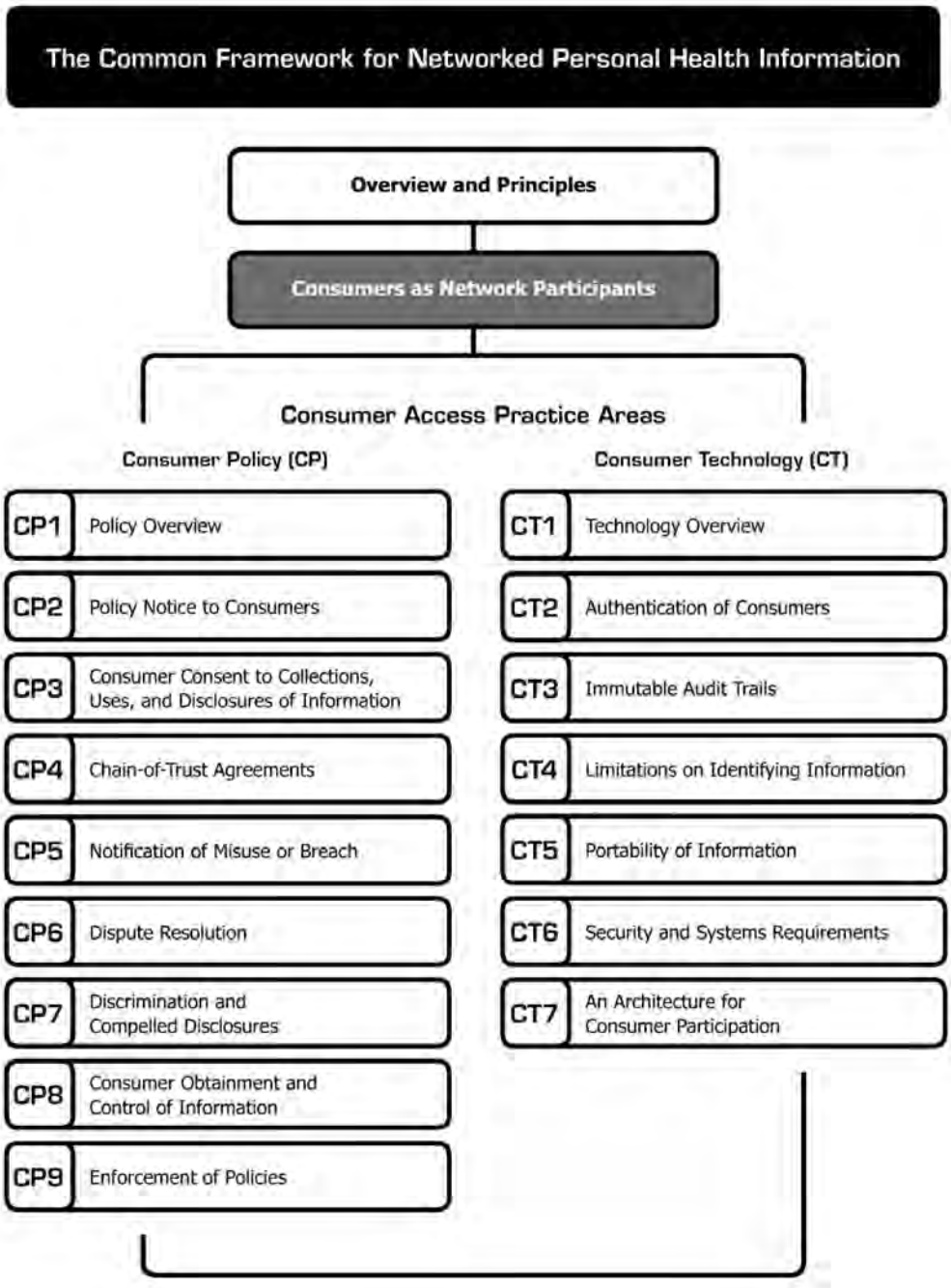
Consumers as Network Participants

Consumers as Network Participants

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:



Consumers as Network Participants*

The average person's ability to access data and communicate electronically is proliferating exponentially. Consumer adoption of digitally networked services has transformed the culture of many industries — often in ways unimaginable barely a decade ago.

Consider these examples of rapid consumer adoption of web-based technologies:

- **Communications:** E-mail is now an indispensable tool of communication for hundreds of millions of people worldwide. Instant messaging and Voice over Internet Protocol (VoIP), such as skype.com, are increasingly accepted alternatives to traditional telephones.
- **Search:** The indexing of online information places enormous research power in the hands of individuals. People now "Google" or "MapQuest" without thinking of picking up a phone book or going to a library. Search engines are exposing ever more granular information, such as full-text searches of vast libraries of books, or the estimated value of your home, or the presence of a registered sex offender next door. Collective contributions by customers add value to search engine results, as demonstrated by the niche "layers" that individuals can add to Google maps.
- **E-commerce:** Web sites such as Amazon, eBay, and Craigslist create ever-expanding communities of buyers and sellers, which in turn create ever-expanding content, inventory, and transactions. Opening up online access to previously proprietary networks, such as real estate listings and flight schedules, has precipitated dramatic new conveniences for consumers and efficiencies for industry.
- **Personal finance:** Consumers embrace ATMs, debit cards, personal finance and tax software, and online banking and investment brokerage services. Such online transactions and self-management tools replace mail, phone, and retail encounters with financial institutions.
- **Entertainment:** The explosive popularity of Apple Computer's iPod represents a progression toward individual manipulation and portability of entertainment media and other data. No longer passive consumers of radio program director decisions, individuals increasingly create and share their own "playlists" and "podcasts." In another example, fantasy sports create networks of enthusiasts more deeply engaged than mere spectators of events.
- **Content:** Perhaps the most interesting techno-social trend is how newly networked consumers generate whole new bodies of content. Bloggers, who use software that makes it easy to self-publish on the web, are directly challenging political and journalistic institutions, among others. People are now pouring their innermost thoughts and images into the worldwide digital stream through online communities, such as MySpace.com and YouTube.com. Wikipedia represents a related and equally powerful trend: online collaborative publishing that derives its authority through the self-regulating nature of open communities. MySpace and Wikipedia in particular illustrate a phenomenal expansiveness of online community content creation. By most accounts,[1,2] both have emerged in about 18 months to join the 20 most popular sites on the web. Wikipedia is

* **Connecting for Health** thanks Josh Lemieux, Markle Foundation; Daren Nicholson, MD, an independent contractor, and David Lansky, PhD, for drafting this paper, parts of which were originally published by the Markle Foundation in December 2006.

now the most frequently visited reference site on the Internet.[3]

This paper does not attempt a comprehensive analysis of such successful innovations in sectors other than health care, but we observe that they share a few basic traits:

1. **They are highly useful.** All of the examples cited above provide rapid utility and convenience by taking available digital data, making it digestible, and providing immediate value to consumers.
2. **They are easy to use.** Web applications that have diffused broadly typically deliver not only high utility, but also a simple user interface that does not limit or burden the consumer.[4]
3. **They are free or inexpensive for consumers to use.** Whether supported through advertisements or not-for-profit foundations, dramatic-growth applications generally collect small or no fees from consumers.
4. **They rapidly proliferate due to the power of networks.** Consumers connect to various networks via their credit cards, cell phones, e-mail accounts, affinity club memberships, and so on. Search engines point to information residing across a vast number of sources, all tied together by the Internet (which itself is a network of networks). Point-to-point communication tools like e-mail and cell phones work because they can slice across competing networks. Credit cards work across competing banks because there are worldwide networks that tie them together. People trust strangers on eBay because there is a trusted payment network, PayPal, as well as a network of buyers and sellers who provide accountability by collectively and publicly rating each other. Sites like Wikipedia, Craigslist, and MySpace have created arrays of communities of people with similar interests.

A key ingredient to the successes cited above is a fresh openness toward consumer access to, and contribution of, information. By contrast, the health care industry has moved more slowly toward providing consumers with online access to health data and interactive services. Personal health information is different — often more complex, scattered, sensitive, less structured — than the other types of information cited above. However, electronic personal health records (PHRs) represent an emerging vehicle to increase consumer participation in the health sector.

Personal Health Records (PHRs)

PHRs encompass a wide variety of applications that enable people to collect, view, manage, or share copies of their health information or transactions electronically. Many PHR applications in existence today facilitate the viewing of health information. A new generation of PHRs promotes the development of multiple and diverse applications that act on personal health information to help users with specific tasks. Although there are many variants, PHRs are based on the fundamental concept of facilitating an individual's access to and creation of personal health information in a usable computer application that the individual (or a designee) controls. We do not envision PHRs as a substitute for the professional and legal obligation for recordkeeping by health care professionals and entities. However, they do portend a beneficial trend toward greater engagement of consumers in their own health and health care.

Today's PHRs are generally "un-networked." They typically require the consumer to enter data manually or get a view of information from a single entity such as one health plan, one pharmacy, or perhaps one health care provider's electronic health record (EHR). Yet most people have relationships with many different doctors and health care entities; particularly those Americans with multiple chronic conditions — more than 60 million today and estimated to reach 81 million by 2020[5] — must coordinate their care across several providers and entities. If the PHR is limited to one particular relationship, it may not meet the long-term needs of many whose information is dispersed

across organizations. Some people in a stable relationship with one integrated delivery system may today have their information adequately accessible through an application from that institution. However, for most people, over time, PHRs would be much more useful if they were networked to aggregate the consumer's health information across multiple sources (e.g., the consumer's insurance eligibility and claims, her records from all of her doctors, her lab results, her pharmacy services, her diagnostic imaging, etc.).

'Networked' PHRs as Tools for Transformation

The mere aggregation of the consumer's data, however, should not be an end in itself. The true test is whether the network makes it easier for ordinary people to coordinate and engage more actively in their own health and health care. We see a networked environment for PHRs as a foundation for Americans to improve the quality and safety of the care they receive, to communicate better with their doctors, to manage their own health, and to take care of loved ones.

This paper argues that consumers can help accelerate transformative change, particularly in a networked information environment. However, we emphasize that clinicians also have a critical role in realizing the full potential of networked PHRs. Consumers continue to see doctors and other health professionals as the key agents of their care and the most trusted hosts of their personal health information. To take advantage of networked personal health information, both consumers and clinicians must be open to changes in their relationships, responsibilities, and workflows. Network-enabled efficiencies and safety improvements are more likely to occur if consumers and health care professionals act as partners who share access to and responsibility for updating personal health information. The status quo — in which most personal health information under the custodianship of providers, payers, and other entities is largely "un-networked" — makes it more difficult for consumers to gather their data from multiple sources, more difficult to choose freely among providers, and thus more difficult to manage their health.

The Rationale for Networking Consumers

Entrenched problems in the American health care system are well-documented. Among the oft-cited deficiencies:

- Fragmentation that leads to inefficiency and duplication of efforts and costs.[6,7]
- Disappointing levels of safety and quality that lead to high rates of medical errors.[8,9,10]
- Frequent unavailability of vital information at point of care.[11]
- High costs that are growing at an unsustainable rate.[12,13]
- An overall lack of patient-centeredness.[14]

Rapid consumer adoption of newly networked services has proven to be possible — indeed phenomenal — in other sectors. Consumers can adapt to technology and culture transformation more rapidly than large health care institutions with long histories of business processes and legacy systems. Furthermore, even as the majority of clinicians continue to keep consumers' data on paper, other important personal health information — namely claims, pharmacy, diagnostic images, and lab data — are available in digital form today. We conclude that the immediate effort to catalyze health care transformation must include a strategy to create a networked environment for PHRs and related technologies that takes advantage of these currently available digital data streams. Providers can gradually form and join networks as their systems increasingly interoperate. In fact, networked connections to PHRs could help accelerate the EHR adoption curve as clinicians see advantages to joining the network.

There are additional strong rationales for involving consumers in a much-needed transformation toward greater information access and transparency. First, the health care consumer has the largest stake in the contents of such information. The consumer's life is put at risk when preventable errors occur due to lack of information. Second, the consumer is the ultimate payer of health care services. Consumers are being asked to pay directly for a larger proportion of their care.[15,16] Third, younger generations expect to use technology in almost all aspects of their lives. Fourth, as the

number and complexity of diagnostic and treatment modalities grows at a rapid pace, patients are increasingly required to share the responsibility of decision-making with their health care providers. Furthermore, patients are often in the best position to gather and share information with providers.[17,18] For example, a physician might know that a medication has been prescribed for a patient. But without asking the patient, the doctor does not know whether the patient actually took the medication, how well it worked, what other remedies she is taking, or whether she had side effects.

Empowering health care consumers by placing information directly in their hands has the potential to radically improve health care.[19,20] PHRs are still in the early development stages, and a great deal of study is needed to measure the benefits and risks of PHRs. Consumers, patients, and their families vary widely in the responsibilities they each wish to maintain in their own health. However, as noted in **Connecting for Health's** 2004 report, *Connecting Americans to Their Health Care*, preliminary evidence suggests that PHRs have potential to:

- Empower patients and their families. [21,22,23,24,25,26,27,28]
- Improve the patient-clinician relationship.[29,30,31,32,33]
- Increase patient safety.[34,35,36,37]
- Improve the quality of care.[38,39,40,41,42]
- Improve efficiency and convenience.[43,44,45,46,47,48]
- Improve privacy safeguards.[49,50]
- Save money.[51,52,53,54,55,56,57]

Lastly, there is general agreement among many stakeholders, including those listed below, that PHRs should be a key part of health care modernization and reform efforts:

- Government bodies, like the National Committee on Vital and Health Statistics[58] and the American Health Information Community.[59]
- Professional societies, such as the American Medical Association[60] and the American Health Information Management Association.[61]
- Consumer groups, such as AARP and the American Diabetes Association.[62]
- Health insurance plan associations, like America's Health Insurance Plans and the Blue Cross Blue Shield Association.[63]
- Bipartisan political leaders.[64]

Addressing Key Policy Concerns Will Be Core to the Transformation Process

Although a networked PHR would provide significant benefits to consumers, the exchange of health data over an electronic network poses serious concerns. Confidentiality of personal health information is a core American value.[65] There is evidence that Americans support a network for health information exchange — if security and confidentiality safeguards are sufficient.[66]

Thus, before encouraging the ubiquitous networking of PHRs to other health information systems, we must establish a common understanding and an adequate set of shared rules. We need a technical approach that allows access controls to keep information flowing among people authorized to see it — and protected from unauthorized access or use. The selection and implementation of technical elements are themselves aids or obstacles to confidentiality and security.

If PHRs can be authorized to connect securely to multiple data streams on the network, then the competition among PHRs will be based on service, features, and value to the consumer, not mere custody of the consumer's data. All of the participants within the networked environment — including health care institutions and professionals, insurance companies, labs, pharmacy services, employers, and consumers themselves — must agree to basic principles for providing individuals the ability to obtain personal health information about them, and security and confidentiality protections must be "baked in" to the network design.

We do not know what kinds of applications and functions will be most effective in encouraging the transformation we seek. The mere presentation of health data to consumers is not as likely to be transformative as new applications to interpret and apply the data in innovative ways that provide specific benefit to

specific people, and connect them with their health team and caregivers. Although the Common Framework for Networked Personal Health Information recommends a framework for enabling networked PHRs, we purposely avoid recommendations on what those applications should be or do. Development of a sufficiently flexible network will enable the use of a great variety of personal health technology applications, including many that we cannot imagine today.

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*

[1] The Washington Post [homepage on the Internet]. Washington: The Washington Post Company; c2006 [cited 2006 May 8]. Top Web Domains; [about 4 screens]. Available at: http://www.washingtonpost.com/wpdyn/content/custom/2006/03/31/CU2006033101136.html.

[2] Boutin P. A Grand Unified Theory of YouTube and MySpace. Slate [serial on the Internet]. 2006 April 28; [cited 2006 May 2]; [about 5 screens]. Available at: http://www.slate.com/id/2140635/.

[3] Clarke G. Wikipedia Eclipses CIA. The Register [serial on the Internet]. 2005 September 7; [cited 2006 May 4]; [about 3 screens]. Available at: http://www.theregister.co.uk/2005/09/07/wikipedia_growth/.

[4] Boutin P. A Grand Unified Theory of YouTube and MySpace. Slate [serial on the Internet]. 2006 April 28; [cited 2006 May 2]; [about 5 screens]. Available at: http://www.slate.com/id/2140635/.

[5] Anderson G. Partnership for Solutions [slide presentation]. 2004; [cited 2006 May 2]. Available at: http://www.partnershipforsolutions.org/DMS/files/anderson_cdc.ppt.

[6] Shi L, Singh D. Essentials of the US Health Care System. Sudbury, MA: Jones and Bartlett Publishers, Inc.; 2004.

[7] Blendon RJ et al. Common Concerns amid Diverse Systems: Health Care Experiences in Five Countries. Health Aff. 2003 May-Jun;22(3):106-21.

[8] Institute of Medicine. To Err is Human, Building a Safer Health System. Washington: National Academies Press; 2000.

[9] McGlynn EA, Asch SM, Adams J, Keesey J, Hicks J, DeCristofaro A, Kerr EA. The Quality of Health Care Delivered to Adults in the United States. N Engl J Med. 2003 June 26;348(26):2635-2645.

[10] Miller MR, Zhan C. Pediatric Patient Safety in Hospitals: A National Picture in 2000. Pediatrics. 2004 Sep;114(3):907.

[11] Connecting for Health. Achieving Electronic Connectivity in Healthcare [monograph on the Internet]. New York: Markle Foundation; 2004 [cited 2006 August 1]. Available at: http://www.connectingforhealth.org/resources/cfh_aech_roadmap_072004.pdf.

[12] Connecting for Health Steering Group and Personal Health Technology Council. Opportunities for CMS Action in Support of Personal Health Records [monograph on the Internet]. New York: Markle Foundation; 2005 [cited 2006 May 17]. Available at: http://www.connectingforhealth.org/resources/CMS_Response_Final_083105.pdf.

[13] OECD [homepage on the Internet]. Paris: OECD; [updated 2004 March 6; cited 2006 June 14]. Health Spending in Most OECD Countries Rises, with the U.S. far Outstripping all Others; [about 4 screens]. Available at: http://www.oecd.org/document/12/0,2340,en2649_201185_31938380_1_1_1_1,00.html.

[14] Institute of Medicine. Crossing the Quality Chasm: A New Health System for the 21st Century. Washington: National Academies Press; 2001.

[15] Robinson J. Health Savings Accounts – The Ownership Society in Health Care. N Engl J Med. 2005 Sep;353(12):1199-1202.

[16] Maze J. Consumerism Creeping into Health Plans. The Post and Courier (Charleston, SC). 2005 December 5, final ed.: E6.

[17] Tang P et al. Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption. J Am Med Inform Assoc. 2006 Mar-Apr;13(2):121-126.

[18] Denton IC. Will Patients use Electronic Personal Health Records? Responses From a Real-Life Experience. J of Healthc Inf Manag. 2001 Fall;15(3):251-259.

[19] Tang P et al. Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption. J Am Med Inform Assoc. 2006 Mar-Apr;13(2):121-126.

[20] American Health Information Management Association [homepage on the Internet]. Chicago: American Health Information Management Association; [updated 2005 July 25; cited 2006 May 8]. AHIMA press release: Personal Health Records belong to the Patient; [about 1 screen]. Available at: http://www.ahima.org/press/press_releases/05.0725.asp.

[21] Masys D, Baker D, Butros A, Cowles KE. Giving Patients Access to their Medical Records via the Internet: The PCASSO Experience. J Am Med Inform Assoc. 2002 Mar-Apr;9(2):181-91.

[22] Jimison HB, Sher PP. Advances in Health Information Technology for Patients. J AHIMA. 1998 Sep;69(8):42-6.

[23] Tang PC, Newcomb C. Informing Patients: A Guide for Providing Patient Health Information. J Am Med Inform Assoc. 1998 Nov-Dec;5(6):563-70.

[24] Winkelman WJ, Leonard KJ. Overcoming Structural Constraints to Patient Utilization of Electronic Medical Records: A Critical Review and Proposal for an Evaluation Framework. J Am Med Inform Assoc. 2004 Mar-Apr;11(2):151-61.

[25] Bluml BM, McKenney JM, Cziraky MJ. Pharmaceutical Care Services and Results in Project ImPACT: Hyperlipidemia. J Am Pharm Assoc (Wash). 2000 Mar-Apr;40(2):157-65.

[26] Broder C. Projects Tap Technology for Disease Management. iHealthBeat [serial on the Internet]. 2003 June 10; [about 3 screens]. Available at: http://www.ihealthbeat.org/index.cfm?Action=dspItem&itemID=99541.

[27] Neville R, Greene A, McLeod J, Tracy A, Surie J. Mobile Phone Text Messaging Can Help Young People Manage Asthma. BMJ. 2002 Sep 14;325(7364):600.

[28] Billault B, DeGoulet P, Devries C, Plouin P, Chattellier G, Menard J. Use of a Standardized Personal Medical Record by Patients with Hypertension: A Randomized Controlled Prospective Trial. MD Comput. 1995 Jan-Feb;12(1):31-5.

[29] Tang PC, Newcomb C. Informing Patients: A Guide for Providing Patient Health Information. J Am Med Inform Assoc. 1998 Nov-Dec;5(6):563-70.

[30] Fierman A, Rosen C, Legano L, Lim S, Mendelsohn A, Dreyer B. Immunization Status as Determined by Patients' Hand-Held Cards vs. Medical Records. Arch Pediatr Adolesc Med. 1996 Aug;150(8):863-6.

[31] MacDonald K. Online Patient-Provider Communication Tools: An Overview [monograph on the Internet]. San Francisco: California Health Care Foundation; 2003 November; [cited 2006 June 15]. Available at: http://www.chcf.org/topics/view.cfm?itemid=21600.

[32] Dishman E, Sherry J. Changing Practices: Computing Technology in the Shifting Landscape of American Healthcare. Santa Clara: Intel Corporation. 1999.

[33] Von Knoop C, Lovich D, Silverstein MB, Tutty M. Vital Signs: E-Health in the United States [monograph on the Internet]. Boston: Boston Consulting Group; 2003 [cited 2006 June 15]. Available at: www.bcg.com/publications/files/Vital_Signs_Rpt_Jan03.pdf.

[34] Kaushal R, Shojania KG, Bates DW. Effects of Computerized Physician Order Entry and Clinical Decision Support Systems on Medication Safety: A Systematic Review. Arch Intern Med. 2003 Jun 23;163(12):1409-16.

[35] Potts AL, Barr FE, Gregory DF, Wright L, Patel NR. Computerized Physician Order Entry and Medication Errors in a Pediatric Clinical Care Unit. Pediatrics. 2004 Jan;113 (1 Pt 1):59-63.

[36] Bennett JW, Glasziou PP. Computerized Reminders and Feedback in Medication Management: A Systematic Review of Randomized Controlled Trials. Med J Aust. 2003 Mar 3;178(5):217-22.

[37] Miller RH, Sim I, Newman J. Electronic Medical Records: Lessons from Small Physician Practices [monograph on the Internet]. San Francisco: California Health Care Foundation; 2003 October [cited 2006 June 15]. Available at: http://www.chcf.org/topics/view.cfm?itemID=21521.

[38] Bluml BM, McKenney JM, Cziraky MJ. Pharmaceutical Care Services and Results in Project ImPACT: Hyperlipidemia. J Am Pharm Assoc (Wash). 2000 Mar-Apr;40(2):157-65.

[39] Tang PC, Newcomb C. Informing Patients: A Guide for Providing Patient Health Information. J Am Med Inform Assoc. 1998 Nov-Dec;5(6):563-70.

[40] Bennett JW, Glasziou PP. Computerized Reminders and Feedback in Medication Management: A Systematic Review of Randomized Controlled Trials. Med J Aust. 2003 Mar 3;178(5):217-22.

[41] Neville R, Greene A, McLeod J, Tracy A, Surie J. Mobile Phone Text Messaging Can Help Young People Manage Asthma. BMJ. 2002 Sep 14;325(7364):600.

[42] Winkelman WJ, Leonard KJ. Overcoming Structural Constraints to Patient Utilization of Electronic Medical Records: A Critical Review and Proposal for an Evaluation Framework. J Am Med Inform Assoc. 2004 Mar-Apr;11(2):151-61.

[43] Huff C. Medical Paperwork Pains: Patients Seeking Records Sometimes Frustrated. Arlington Star-Telegram (Fort Worth, TX). 1999 January 11: 1B, 5B.

[44] Miller RH, Sim I, Newman J. Electronic Medical Records: Lessons from Small Physician Practices [monograph on the Internet]. San Francisco: California Health Care Foundation; 2003 October [cited 2006 June 15]. Available at: http://www.chcf.org/topics/view.cfm?itemID=21521.

[45] Bluml BM, McKenney JM, Cziraky MJ. Pharmaceutical Care Services and Results in Project ImPACT: Hyperlipidemia. J Am Pharm Assoc (Wash). 2000 Mar-Apr;40(2):157-65.

[46] MacDonald K. Online Patient-Provider Communication Tools: An Overview [monograph on the Internet]. San Francisco: California Health Care Foundation; 2003 November; [cited 2006 June 15]. Available at: http://www.chcf.org/topics/view.cfm?itemid=21600.

[47] RelayHealth. The RelayHealth WebVisit Study: Executive Summary [monograph on the Internet]. Emeryville, CA: Relay Health; 2002 [cited 2006 June 15]. Available at: https://www.relayhealth.com/rh/general/aboutUs/studyResults.aspx.

[48] Von Knoop C, Lovich D, Silverstein MB, Tutty M. Vital Signs: E-Health in the United States [monograph on the Internet]. Boston: Boston Consulting Group; 2003 [cited 2006 June 15]. Available at: www.bcg.com/publications/files/Vital_Signs_Rpt_Jan03.pdf.

[49] Masys D, Baker D, Butros A, Cowles KE. Giving Patients Access to their Medical Records via the Internet: the PCASSO experience. J Am Med Inform Assoc. 2002 Mar-Apr;9(2):181-91.

[50] Schoenberg R, Safran C. Internet-Based Repository of Medical Records that Retains Patient Confidentiality. BMJ. 2000 Nov 11;321(7270):1199-203.

[51] Gawthorn E. Introducing the Personal Health Record: RACGP Health Record System [Brochure]. South Melborne, Australia: Royal Australian College of General Practitioners; 1982.

[52] Miller RH, Sim I, Newman J. Electronic Medical Records: Lessons from Small Physician Practices [monograph on the Internet]. San Francisco: California Health Care Foundation; 2003 October [cited 2006 June 15]. Available at: http://www.chcf.org/topics/view.cfm?itemID=21521.

[53] Von Knoop C, Lovich D, Silverstein MB, Tutty M. Vital Signs: E-Health in the United States [monograph on the Internet]. Boston: Boston Consulting Group; 2003 [cited 2006 June 15]. Available at: www.bcg.com/publications/files/Vital_Signs_Rpt_Jan03.pdf.

[54] Bluml BM, McKenney JM, Cziraky MJ. Pharmaceutical Care Services and Results in Project ImPACT: Hyperlipidemia. J Am Pharm Assoc (Wash). 2000 Mar-Apr;40(2):157-65.

[55] Broder C. Projects Tap Technology for Disease Management. iHealthBeat [serial on the Internet]. 2003 June 10; [about 3 screens]. Available at: http://www.ihealthbeat.org/index.cfm?Action=dspItem&itemID=99541.

[56] MacDonald K. Online Patient-Provider Communication Tools: An Overview [monograph on the Internet]. San Francisco: California Health Care Foundation; 2003 November; [cited 2006 June 15]. Available at: http://www.chcf.org/topics/view.cfm?itemid=21600.

[57] RelayHealth. The RelayHealth WebVisit Study: Executive Summary [monograph on the Internet]. Emeryville, CA: Relay Health; 2002 [cited 2006 June 15]. Available at: https://www.relayhealth.com/rh/general/aboutUs/studyResults.aspx.

[58] National Committee on Vital and Health Statistics [homepage on the Internet]. Washington: Department of Health and Human Services; [updated 2005 September 9; cited 2006 May 8]. September 9, 2005 Letter to Secretary Leavitt on Personal Health Record (PHR) Systems; [about 16 screens]. Available at: http://www.ncvhs.hhs.gov/050909lt.htm.

[59] United States Department of Health and Human Services [homepage on the Internet]. Washington: United States Department of Health and Human Services; [updated 2006 May 3; cited 2006 May 8]. American Health Care Community Consumer Empowerment Workgroup; [about 2 screens]. Available at: http://www.hhs.gov/healthit/ahic/ce_main.html.

[60] American Medical Association [homepage on the Internet]. Chicago: American Medical Association; c1995-2005 [cited 2006 May 8]. Policy H-185.979 allocation of health services; [about 1 screen]. Available at: http://www.ama-assn.org/apps/pf_new/pf_online?f_n=browse&p_p=T&&s_t=&st_p=&nth=1&prev_pol=policyfiles/HnE/H-185.979.HTM&nxt_pol=policyfiles/HnE/H-185.982.HTM&.

[61] American Health Information Management Association [homepage on the Internet]. Chicago: American Health Information Management Association; [updated 2005 July 25; cited 2006 May 8]. AHIMA press release: Personal Health Records belong to the Patient; [about 1 screen]. Available at: http://www.ahima.org/press/press_releases/05.0725.asp.

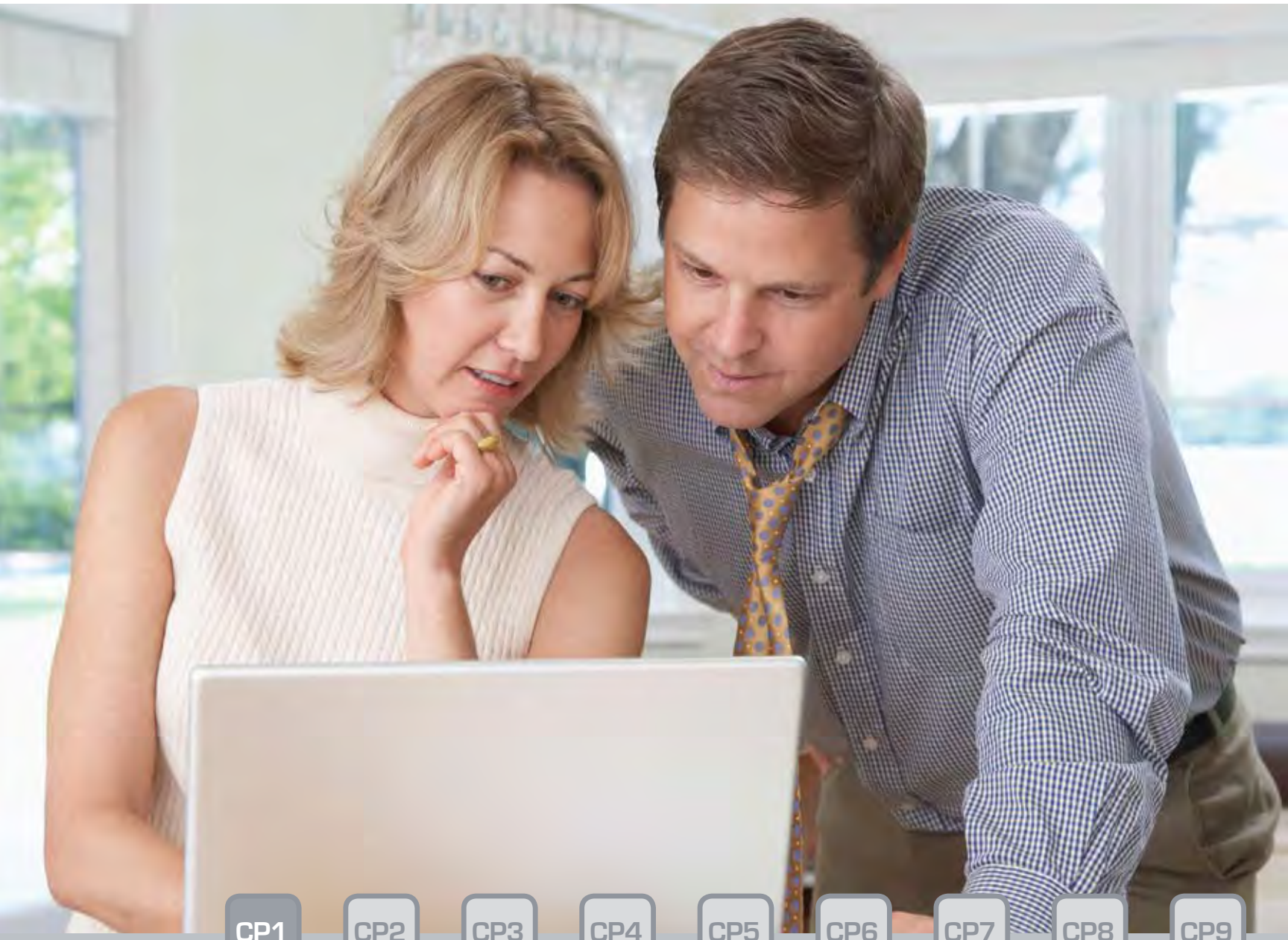
[62] Cerner Corporation [homepage on the Internet]. Kansas City: Cerner Corporation; c2006 [updated 2004 October 12; cited 2006 June 20]. Cerner press release: Cerner Launches $25-Million, 10-Year Initiative to Provide Personal Health Records to Kids with Diabetes; [about 3 screens]. Available at: http://www.cerner.com/public/NewsReleases.asp?id=257&cid=228.

[63] America's Health Insurance Plans [homepage on the Internet]. Washington: America's Health Insurance Plans; [updated 2006 January 31; cited 2006 May 8]. AHIP Statement on the State of the Union Address; [about 3 screens]. Available at: http://www.ahip.org/content/pressrelease.aspx?docid=14738.

[64] California Healthline [homepage on the Internet]. Washington: Advisory Board Company; [updated 2005 May 10; cited 2006 May 8]. Former House Speaker Newt Gingrich Calls for Increased Investment in Health Care Information Technology; [about 2 screens]. Available at: http://www.californiahealthline.org/index.cfm?Action=dspItem&itemID=111090&ClassCD=CL108.

[65] Connecting for Health. The Architecture for Privacy in a Networked Health Information Environment [monograph on the Internet]. New York: Markle Foundation; 2006 [cited 2006 May 17]. Available at: http://www.connectingforhealth.org/commonframework/docs/P1_CFH_Architecture.pdf.

[66] Markle Foundation. Markle Foundation Survey Fact Sheet [monograph on the Internet]. New York: Markle Foundation; 2005 [cited 2006 May 17]. Available at: http://www.connectingforhealth.org/resources/101105_survey_summary.pdf.



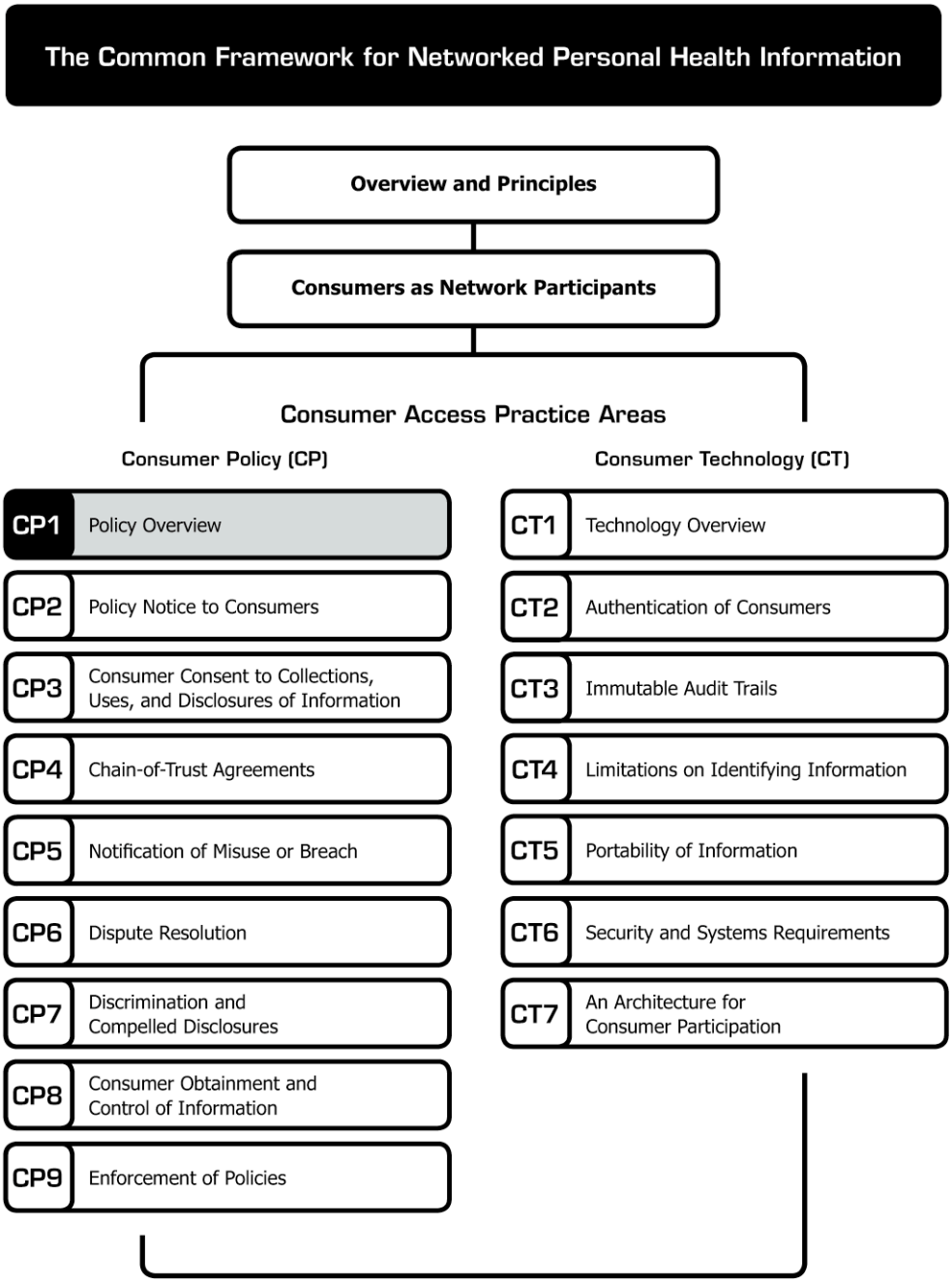
Policy Overview

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.

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.)

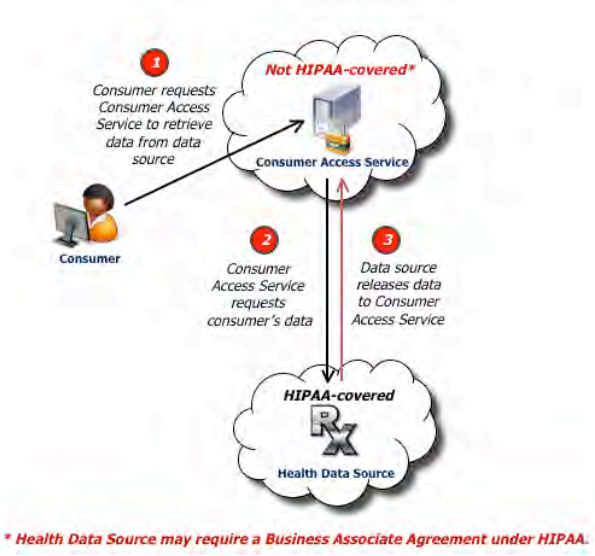
Thus, if a Covered Entity provides a Consumer Access Service to its patients, members, or employees, then the Covered Entity must comply with Privacy Rule requirements (even if the actual service is supplied by a vendor under a Business Associate agreement). However, if the Consumer Access Service is 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.).



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.*

CP1 CP2 CP3 CP4 CP5 CP6 CP7 CP8 CP9

CT1 CT2 CT3 CT4 CT5 CT6 CT7

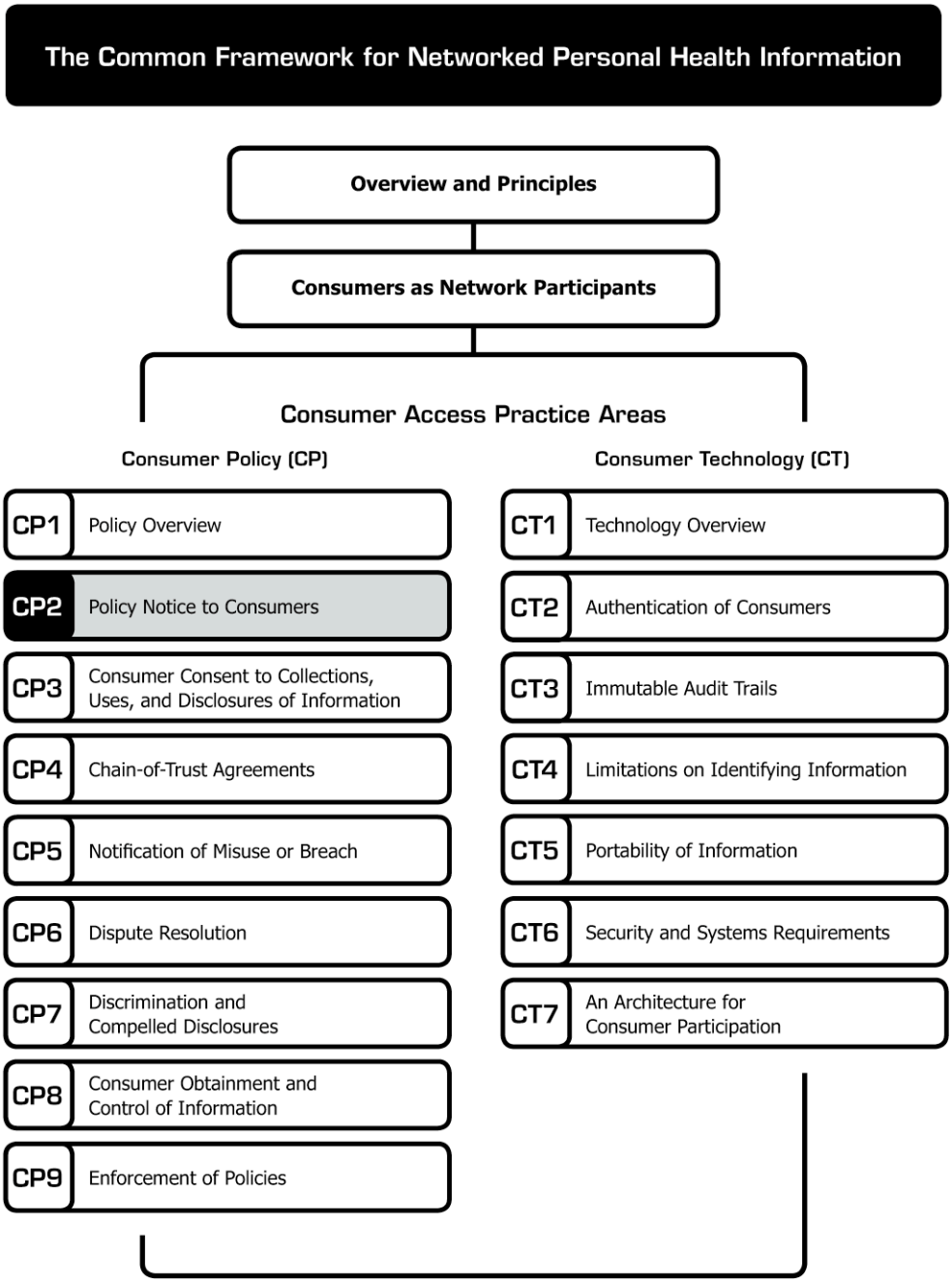
Policy Notice to Consumers

Policy Notice to Consumers

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 Notice to Consumers*

Purpose: There is general agreement that "good privacy begins with effective transparency"[1] and that consumers must be given access to information about policies for collection, use, and disclosures of personal health information, including privacy and security practices, terms and conditions of use, and other relevant policies.

It is an industry standard to post a privacy policy for online services.[2] In practice, however, there are several limitations to the effectiveness of policy notices to consumers, the most important being that consumers rarely read them (and the few who do often find them confusing). Please see **Appendix A** for a discussion of the limitations of notice and consent in today's Internet environment.

Despite the well-known limitations with current practice in implementing the openness and transparency principle, there are at least three essential and practical reasons to develop and post clear policies on privacy and terms of use:

1. Even if most consumers fail to read them, the interested consumer has the right to know what he or she is agreeing to.
2. The process of developing and promulgating public policies for health data custodianship helps organizations examine their internal policies, and correct shortcomings, if necessary.[3]
3. The posting of publicly available policies brings into play various state and federal laws and regulations that can help police the industry and provide a layer of protection to consumers. If an entity adopts a privacy policy in the absence of a legal requirement to do so, and that policy is publicly available, it is likely to be enforceable if breached through the Federal Trade Commission as "unfair or deceptive practice." Once an entity makes a policy available to its customers and patients, it makes itself accountable for adhering to those policies.

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

1. Openness and transparency

2. Purpose specification

3. Collection limitation and data minimization

4. Use limitation

* "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] The Center for Information Policy Leadership, Hunton & Williams, LLP, *Ten Steps to Develop a Multilayered Privacy Notice*. February 14, 2006, page 1. Available at: http://www.hunton.com/files/tbl_s47Details/FileUpload265/1405/Ten_Steps_whitepaper.pdf.

[2] *TRUSTe, Your Online Privacy Policy,* White Paper. 2004, p. 5-6. Accessed online on August 16, 2007, at the following URL: http://www.truste.org/pdf/WriteAGreatPrivacyPolicy.pdf.

[3] *TRUSTe, Your Online Privacy Policy*, White Paper. 2004, page 6. Accessed online on August 16, 2007, at the following URL: http://www.truste.org/pdf/WriteAGreatPrivacyPolicy.pdf.

Consumers would be better served if there were an industry-standard online format for notice of data-handling and privacy practices. We would like to see a public-private collaborative, including industry and consumer representatives as well as web accessibility and disability experts, work on such a standardized format that would enable a general, apples-to-apples comparison across consumer-accessible health applications. Such an effort should begin with the FTC's Fair Information Practice Principles as well as the documents summarized in **Appendix A**. We offer the following as guidelines.

Recommended Practice:

PHRs and Consumer Access Services must develop privacy policies, terms and conditions of use, and other relevant policies related to the handling of health information. Such statements should be:

1. **Clearly written:** Avoid excessive jargon. To the extent possible, target 4th to 6th grade reading ability. To the extent practical, provide notice in the language(s) of the target populations.
2. **Comprehensive:** Answer the questions raised by the nine **Connecting for Health** core principles. *(See **Overview and Principles**.)* The consumer should be able to know what, how, and why information is collected, used, or shared, as well as how long it will be kept, how the consumer can exercise choices or controls over the information, and whether it can be disputed or deleted, and what procedures, if any, are in place to notify affected people in the event of breach. Policy notices should define what the Consumer Access Services consider to be personally identifying information (PII) and what information is not considered personally identifying. For the latter, notice must be clear regarding limits on the ability of Consumer Access Services or third parties to make the information "re-identifiable," such as by combining it with other databases. *(See **CT4: Limitations on Identifying Information**.)* Policy notices should provide information about whether personal information will be stored in foreign countries, or whether information collected through the Consumer Access Service will be combined with other information about the individual collected from other sources, services, or contexts. It should also spell out the organization's general policy for complying with reasonable law enforcement requests for disclosure of personal information without the consumer's consent. **Appendix B** provides a more detailed list of possible topics to consider for inclusion in policy notices to consumers.
3. **Summarized:** Present key policies and protections in summary form. Make any necessary additional detail easily accessible. For example, if additional detail is necessary, let the consumer easily click from a summarized version to a more detailed version, and vice versa. It is valuable to test different formats to reach target populations. In some cases, video or other visual or interactive techniques may be more effective than written documents.
4. **Focused on protections:** Do not merely present what the service is permitted to do. Make clear the limitations on what it will do. Refer to the nine privacy principles above.
5. **Easily accessible:** Make links to relevant policies part of the service's global navigation, footer, or other standard location for such policies (i.e., accessible from every page on the site). Post links to policies on the home page and on appropriate screens on which the consumer sets up an account or makes key decisions. Brief policy notices that relate to specific choices, and that appear at the point consumers are exercising those choices, may be more effective than long legal statements that cover many different practices and activities.

6. **Updated:** Provide adequate notice to consumers of modifications in policies. Notices of modification should specifically identify the changes made. We offer the following as preferred practices:

    a. **Versions:** Post each version of the terms of use and privacy policy with identification of version number and effective date. Specifically identify the changes made to the previous version. Retain a record of all dates and means of posting notices of changes.

    b. **Type of notice:** Each time the policies are modified, consider whether it is appropriate to obtain a new authorization from the consumer. Additional authorizations should be obtained in connection with policy modifications that materially alter the policies. Provide users with a meaningful opportunity to review material modifications regardless of whether a new authorization is required.

        - **Non-material changes:** To the extent changes do not affect material provisions of the terms of use and privacy policy, the Consumer Access Service may change such policies at any time and for whatever purpose with or without a new authorization. Notice to the user may take the form of general notice of change regarding non-material provisions of terms of use or privacy policy posted prominently on web site. In this case of non-material changes, continued use of the site under the initial authorization signifies user's consent to new terms and/or policies.
        - **Material changes:** Present consumers with appropriate notice and an option to consent to updated policies if such policies are changed in a way that materially affects their provisions or there is a material change in the business relationship (e.g., a merger, acquisition, or change of ownership of the service). Notice in such cases should be posted prominently in the end-user application (e.g., PHR). It is best practice to send an e-mail to registered users notifying them of material changes, and/or provide notice and an appropriate consent mechanism upon the user's subsequent login. Determining the appropriate consent mechanism may hinge on several factors, including the usability of the interface and the principle that consent should be "proportionate" (i.e., the more sensitive or personally exposing the changes to policy, then the more specific and discrete the mechanism to capture a consumer's consent, and vice versa). *(See **CP3: Consumer Consent to Collections, Uses, and Disclosures of Information**.)* When a Consumer Access Service seeks a new authorization, it should clearly explain the consequences of opting-in and opting-out of the new policies. For example, opting-out may require the consumer to terminate use of the Consumer Access Service. In such cases, the Consumer Access Service should provide the consumer with an easy process for both downloading and printing the user's records. *(See **CP8: Consumer Obtainment and Control of Information** and **CT5: Portability of Information**.)*

Appendix A:
Limitations of Relying on Notice and Consent

The Federal Trade Commission's Fair Information Practice Principles declare:

> The most fundamental principle is notice. Consumers should be given notice of an entity's information practices before any personal information is collected from them. Without notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information.[4]

However, current industry practices of posting policy notices provide only limited protection for even the most careful consumer. We conducted an in-depth analysis of the privacy and terms of use statements of eight different PHR products, chosen based on their relatively high levels of sophistication in data integration. The organizations studied included three large integrated delivery networks, a nationwide insurance company, a nationwide retail pharmacy company, and three independent companies offering PHRs with advertised capabilities to import professionally sourced health data for the consumer. The examination, based on publicly posted policies between June and August 2007, found challenges that will be familiar to any consumer who has signed up for software or services involving personal information over the web:

- Organizations present significantly varying degrees of purpose specification, collection, and use limitations, and offer varying granularity of individual participation and control options.
- Those differences are very difficult to compare from one site to another because the posted policies are not standardized or organized in common formats.
- Policies are typically lengthy and complex, with fine print that may be vague, highly technical, or both.
- Policies contain multiple notices about how personal data will be handled. For example, in at least one case, protections listed in an organization's privacy policy could be changed under its terms and conditions of use (both of which must be agreed to by the consumer).
- Ideally, terms and conditions would be a helpful guide to consumers, spelling out the responsibilities and protections to be undertaken by each party. However, the terms and conditions we examined were typically written from the standpoint of limiting the company's liability and obtaining broad authorization from the consumer. In fine print, for example, we found clauses that allowed disclosure of personal health information to an employer at the request of a consumer's health plan, and or a denial of accountability or redress in the event of a misuse of personal data by contracted third-party entities (i.e., a lack of "chain-of-trust" reassurances).

Other studies have had similar findings. For example, one study that looked at 60 financial privacy notices and found that most were "written at a 3rd-4th year college reading level, instead of the junior high school level that is recommended for materials written for the general public [suggesting] consumers will have a hard time understanding the notices because the writing style uses too many complicated sentences and too many uncommon words."[5] A 2002 study found that none of 80 health web sites examined had a privacy policy that would be "comprehensible to most English-speaking adults in the United States."[6] A recent study, commissioned by the American Health Information Community, examined 30 PHR privacy policies and found them to be "inconsistent" and "incomplete," noting a

[4] Federal Trade Commission, *Fair Information Practice Principles*. Accessed online on August 16, 2007, at the following URL: http://www.ftc.gov/reports/privacy3/fairinfo.shtm.

[5] Hochhauser, Ph.D, *Lost in the Fine Print: Readability of Financial Privacy Notices*. July 2001. Accessed online on August 21, 2007, at the following URL: http://www.privacyrights.org/ar/GLB-Reading.htm.

[6] J Fam Pract 2002: 51:642-645, *Reading Level of Privacy Policies on Internet Health Web Sites - Brief Report*. Accessed online on August 16, 2007, at the following URL: http://findarticles.com/p/articles/mi_m0689/is_7_51/ai_88999808.

general lack of specificity on uses and disclosures of information.[7]

The net result of such practices is an undue burden on consumers to determine what the policies say and do not say. It is not surprising that most consumers do not read online privacy or terms of use statements.[8] It's not uncommon for consumers to later be surprised by unwelcome consequences.[9] This is deeply challenging in an infant industry that requires consumer trust to survive.

It is also important to note that notice alone does not protect consumers. As evidenced by recent FTC and State Attorney General cases, a company may still be engaging in unfair practices even when providing notice to the consumer if that practice could cause significant injury and is buried deeply in a disclosure.[10]

[7] Altarum, *Review of Personal Health Record (PHR) Service Provider Market: Privacy and Security*. January 5, 2007, page 17. Accessed online on August 16, 2007, at the following URL: http://www.hhs.gov/healthit/ahic/materials/01_07/ce/PrivacyReview.pdf.

[8] The Pew Internet & American Life Project, Fox, Rainie, et al.,*The Online Health Care Revolution: How the Web Helps Americans Take Better Care of Themselves*. November 26, 2000. Accessed online on August 21, 2007, at the following URL: http://www.pewinternet.org/pdfs/PIP_Health_Report.pdf.

[9] CNET News.com, *PC Invaders*. April 12, 2002. Accessed online on August 16, 2007, at the following URL: http://news.com.com/2009-1023-885144.html.

[10] See Center for Democracy and Technology, *Spyware Enforcement*, Report. Accessed online on October 22, 2007, at the following URL: http://www.cdt.org/privacy/spyware/20060626spyware-enforcement.php citing several case studies of unfair practices buried in End User License Agreements and privacy notices, including FTC v. Odysseus Marketing, Inc, and Walter Rines, FTC Docket #042-3205; In the matter of Advertising.com, Inc. a/d/b/a Teknosurf.com, and John Ferber, FTC Docket #042-3196; and State of New York v. Direct Revenue, LLC, and Joshua Abram, Alan Murray, Daniel Kaufman, Rodney Hook.

Appendix B:
A Survey of Recommended Areas for Policy Notice to Consumer

The Federal Trade Commission's Fair Information Practice Principles are an essential starting point for online policy notice statements for consumers. The FTC's notice principle reads:

> While the scope and content of notice will depend on the entity's substantive information practices, notice of some or all of the following have been recognized as essential to ensuring that consumers are properly informed before divulging personal information:
>
> - identification of the entity collecting the data;
> - identification of the uses to which the data will be put;
> - identification of any potential recipients of the data;
> - the nature of the data collected and the means by which it is collected if not obvious (passively, by means of electronic monitoring, or actively, by asking the consumer to provide the information);
> - whether the provision of the requested data is voluntary or required, and the consequences of a refusal to provide the requested information; and
> - the steps taken by the data collector to ensure the confidentiality, integrity, and quality of the data.
>
> Some information practice codes state that the notice should also identify any available consumer rights, including: any choice respecting the use of the data; whether the consumer has been given a right of access to the data; the ability of the consumer to contest inaccuracies; the availability of redress for violations of the practice code; and how such rights can be exercised.
>
> In the Internet context, notice can be accomplished easily by the posting of an information practice disclosure describing an entity's information practices on a company's site on the Web. To be effective, such a disclosure should be clear and conspicuous, posted in a prominent location, and readily accessible from both the site's home page and any web page where information is collected from the consumer. It should also be unavoidable and understandable so that it gives consumers meaningful and effective notice of what will happen to the personal information they are asked to divulge.[11]

The following table examined documents from six organizations that have studied items that should be disclosed in a notice statement to consumers. An “X” indicates that the organization has recommended that the item be part of the notice to consumers. This table is for reference only; it does not constitute a recommendation for an industry standard notification form:

[11] Federal Trade Commission, *Fair Information Practice Principles*. Accessed online on August 16, 2007, at the following URL: http://www.ftc.gov/reports/privacy3/fairinfo.shtm.

Privacy Policy Element	ASTM	TRUSTe	URAC	OECD	Nym	H&W
TRANSPARENCY						
What organization is responsible for the information that the consumer provides?			X		X	
Does this privacy policy apply to personal information collected by phone, mail, fax, in-person encounter, or just online through the web site?					X	
What is considered personal information?					X	
Does the organization collect personally identifiable information?				X		
What personally identifiable information is collected?		X	X	X	X	X
How is personally identifiable information collected?				X	X	X
Why is this information collected?						
Are individuals aware that their personal data are being collected?				X		
Who in the organization is responsible for deciding what personal data are collected and how?				X		
Who controls personal data once they are collected?				X		
What choices are available to users regarding collection, use, and distribution of the information?	X	X			X	X
Does the organization have standards, guidelines, and regulations which apply to your collection and use of personal data?				X		
Does the organization allow visitors access to the personal data it has about them?				X		
Does the consumer have opportunities to access and make corrections related to the information, either because of requirements in law or policy in the organization?	X		X		X	X
Are there any limitations on amendment, deletion, or removal of information?			X			
Does the organization use passive tracking mechanisms and if so, why?			X			
What is the organization's business model?	X					

Privacy Policy Element	ASTM	TRUSTe	URAC	OECD	Nym	H&W
APPROPRIATE USE						
Are personal data disclosed to third parties, and if so, why?			X	X	X	X
How and where are data disclosed to third parties stored?				X		X
What personally identifiable information do third parties collect through the web site?		X				
What organization(s) collects the information?		X				
How does the organization use the information?	X	X	X	X	X	X
With whom may the organization share user information?	X	X				
How long is the information kept?	X		X			X
How is the information destroyed?	X					X
What is the policy concerning use of the PHR by individuals other than the consumer (i.e., proxies, providers)?	X					
Who can alter data in the PHR?	X					
What happens to the data in the event of the supplier's merger, acquisition, or dissolution?	X					
What is the policy for transferring the consumer's information to another site?	X					
To what extent is the consumer's information used for data-mining?	X					
Are de-identified data shared with third parties, and if so, what choices does the consumer have regarding these practices?						
How are requests for data from law enforcement and public health agencies handled?						
DATA QUALITY AND ACCURACY						
What are the quality assurance policies concerning the data?	X					
SECURITY AND ACCOUNTABILITY						
What are the measures the organization takes to protect the information under its control?	X	X				
What happens if a visitor has a query about their personal data? What if they are not satisfied with how the organization deals with their query?				X		
What internal and external audit practices does the organization follow?	X					
Can the consumer access audit data?						
ENFORCEMENT						
What mechanisms are in place to ensure that the privacy policy is enforced?						
What mechanisms are in place to provide remedies when there are security breaches or other violations of privacy?						

Sources:

TRUSTe: Your Online Privacy Policy, Whitepaper. 2004. Page 14. Available at: http://www.truste.org/pdf/WriteAGreatPrivacyPolicy.pdf.

OECD: Available at: http://www.oecd.org/document/1/0,2340,en_2649_34255_28863233_1_1_1_1,00.html.

URAC: *Health Web Site Accreditation Standards, 2.0*. Available at: http://accreditnet.urac.org/public/ProgramGuideLight.aspx?l=1&pg=131 Username: ProgramGuide; Password: URACPG16.

Nymity: *Nymity's Short Notice Guide*. Available at: http://www.nymity.com/about_us/documents/NymitysShortNoticeGuide.pdf.

Hunton & Williams,*Ten Steps to Develop a Multilayered Privacy Notice*. Available at: http://www.hunton.com/files/tbl_s47Details/FileUpload265/1405/Ten_Steps_whitepaper.pdf.

ASTM,*Standard Specification for Relationship Between a Person (Consumer) and a Supplier of an Electronic Personal (Consumer) Health Record.* Available at: http://www.astm.org/cgi-bin/SoftCart.exe/DATABASE.CART/REDLINE_PAGES/E2211.htm?E+mystore.

Another useful resource is the work of the W3 Platform for Privacy Preferences (P3P) Project. Although its work has been suspended, P3P made an important contribution toward creating a machine-readable standard for expressing privacy preferences. See http://www.w3.org/P3P/.

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

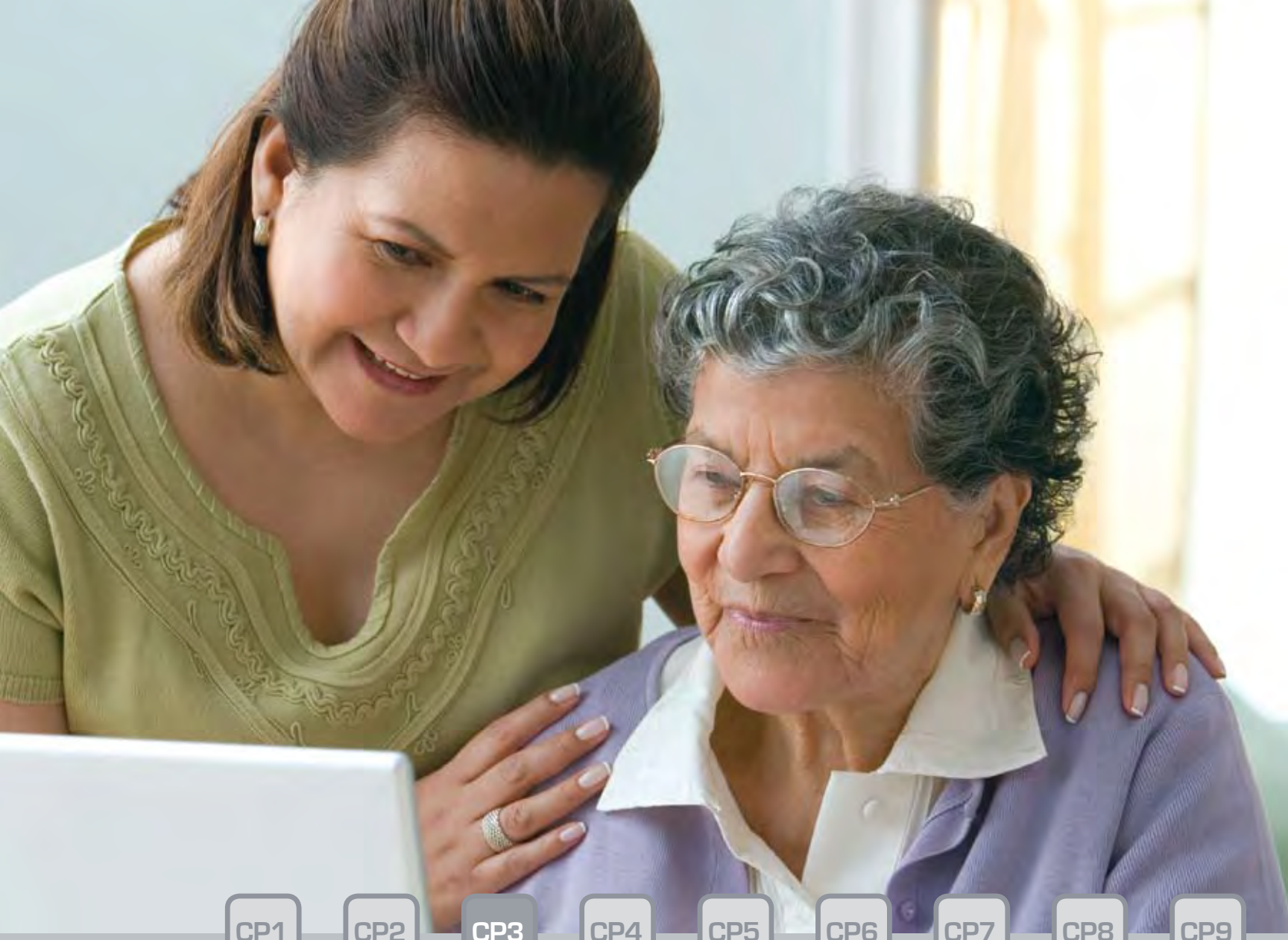
Marcy Wilder, JD, Hogan & Hartson LLP

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.*



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

CT1 CT2 CT3 CT4 CT5 CT6 CT7

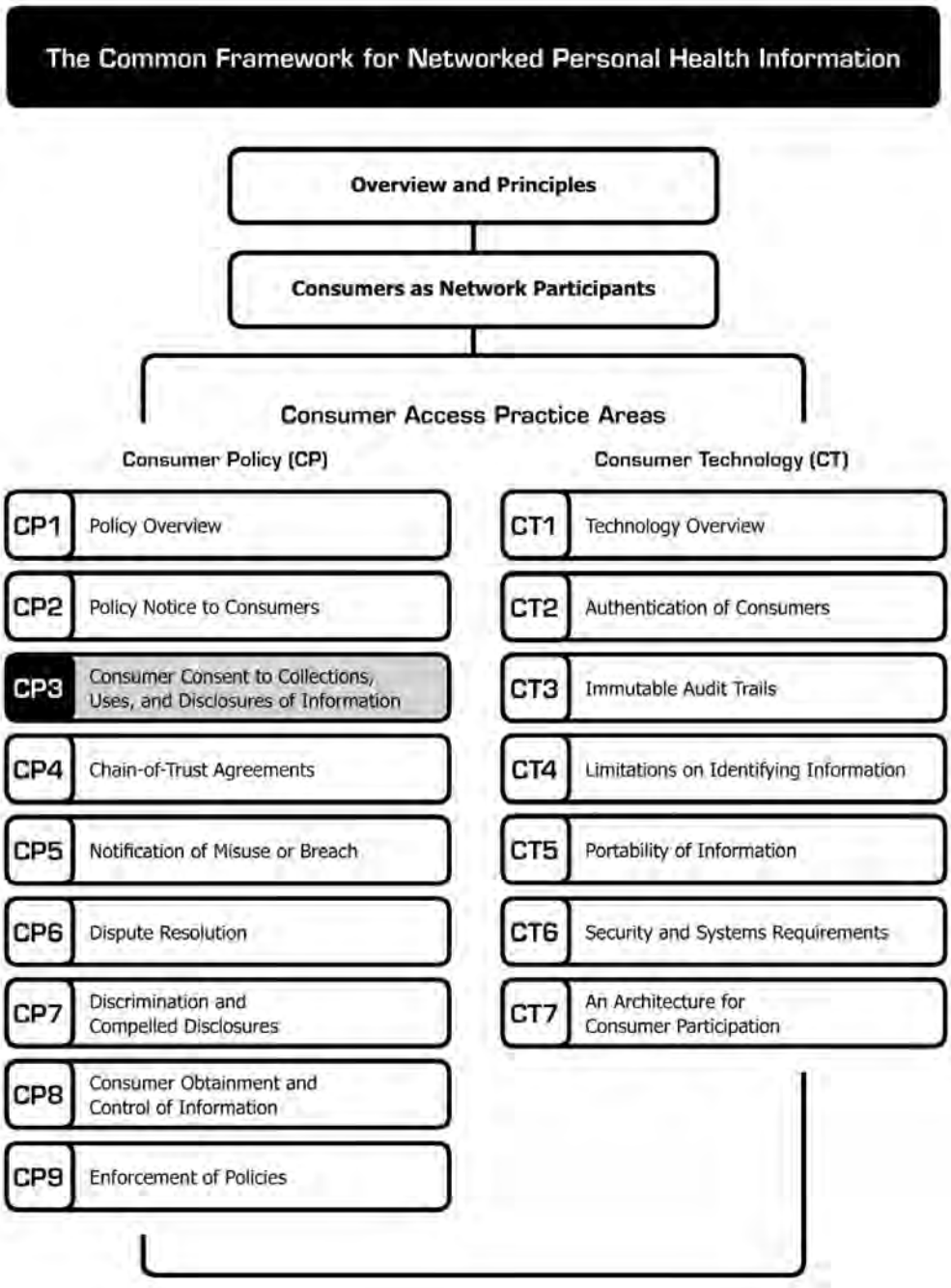
Consumer Consent to Collections, Uses, and Disclosures of Information

Consumer Consent to Collections, Uses, and Disclosures 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 Consent to Collections, Uses, and Disclosures of Information*

Purpose: Consumer-specific data is central to business in the Internet Age. At the same time, consumers continue to express deep concerns about privacy. Understanding acceptable practices to consummate the consumer's consent is thus a critical component of a trusted electronic network.

We note, however, that today's consent practices provide generally weak protection for the average consumer. This is due not only to the largely indecipherable notice statements and consent forms but also to advancing technologies and all of the complexities of health data streams and the legal and business environments discussed in the previous two chapters. Simply put, it is hard for consumers to know what they are consenting to on the Internet. Consent mechanisms, therefore, are *necessary but insufficient by themselves* to ensure the trustworthiness of consumer data streams. A consumer-protective approach includes all of the principles and practices outlined in the Common Framework. The combined practice areas are designed to protect against abuses regardless of whether consent has been obtained.

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

2. Purpose specification

3. Collection limitation and data minimization

4. Use limitation

5. Individual participation and control

* "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.

Still, a fundamental characteristic of PHRs is that they should be voluntary and controlled by the consumer. The consumer should choose whether to open a PHR account. The consumer should choose what entities may access or exchange information into or out of that account.[1] Consent mechanisms, therefore, are *necessary but insufficient* to ensure the trustworthiness of consumer data streams.

* **Connecting for Health** thanks Josh Lemieux, Markle Foundation, for drafting this paper. A special thanks to Marcy Wilder, JD, Hogan & Hartson LLP, and Joy Pritts, JD, Center on Medical Record Rights and Privacy, Health Policy Institute, Georgetown University, for providing extra reviews of this paper.

[1] Markle Foundation, *Connecting Americans to Their Healthcare: Working Group on Polices for Electronic Information Sharing Between Doctors and Patients, Final Report*. July 2004, p. 83-4. Available online at: http://www.connectingforhealth.org/resources/wg_eis_final_report_0704.pdf.

Consent[2] is the process of obtaining permission from an individual to use or disclose her personal information for specified purposes. By defining the bounds of what is permissible, the process of asking for consent should be viewed as providing protection both to consumers and to other participants of a network. It is also an opportunity to educate consumers about the service, its potential benefits, its boundaries, and its risks.

The optimal process for capturing meaningful consent, and its merits as a protection to consumers, remains the subject of much debate. In general terms, the debate has focused on whether consent should be "opt-in" or "opt-out." These are too often polarizing and imprecise terms that have limited value in establishing a broad framework of policies that protect the privacy of health information. In fact, the framing of the "opt-in" or "opt-out" user-interface is as important a decision as determining whether to choose one over the other.[3] Nonetheless, we discuss them here as they are the "terms of art" for the issues related to consent.

Opt-in assumes a refusal of consent unless the consumer specifically indicates otherwise (usually through a formal consent-granting process). Opt-out assumes consent unless the consumer specifically refuses (usually through a formal consent-refusal process). In online environments, such processes are typically presented as checkboxes that the consumer must click to exercise choices.

Definitions for this Appendix

Collection: Any gathering of information as part of a Consumer Access Service. It may include information self-generated by the consumer. It also may include data from professional or other sources (e.g., doctors, labs, pharmacy services, imaging centers, ancillary services, medical devices, etc.)

Use: This includes all uses. We purposely avoid the term "secondary uses" — often described as uses of personal information for purposes other than those for which it was initially collected. Examples of uses of data include storage by the consumer as well as research, public health, or marketing activities by other authorized entities. Each use of information should be described specifically, rather than labeled as "primary" or "secondary."

Disclosures: This includes passing of the consumer's data to a third-party.

We recommend consent mechanisms that address the specific uses of personal health information, its sensitivity to the consumer, and the potential benefits and risks of its disclosure and use. The following questions help determine preferred practice:

[2] For simplicity in this text, we make no distinction between "choice" and "consent." Others have noted a distinction, however. For example, Pricilla Regan wrote: "The concept of consent has long been important in liberal political thought generally (the consent of the governed), as well in many contractual settings (informed consent for medical treatment). Consent implies an active, affirmative agreement of the individual to engage in the activity in question. It also implies that the individual have some understanding of the implications of what is being consented to. The concept of choice has different philosophical roots and practical implications. Choice is an important component of individual autonomy as reflected in the Supreme Court's decisions on reproductive privacy – the ability to choose or decide for oneself. Choice also has roots in market theories of consumer behavior and these roots provide much of the rationale and expectations underlying choice as a fair information practice. In the market setting, adequate information to make a choice is also important, but the information is often framed in terms of benefits and costs derived from choices. Choice addresses the rational, economic individual while consent addresses the political, social individual."

Center for Democracy and Technology, Regan, *The Role of Consent in Information Privacy Protection, Considering Consumer Privacy.*. March 2003, page 24. Accessed online on August 21, 2007, at the following URL: http://www.cdt.org/privacy/ccp/ccp.pdf.

[3] See Steven Bellman, Eric J. Johnson, Gerald Lohse, *To Opt-In Or To Opt-Out? It Depends on the Question*. November 13, 2000. Accessed online on October 22, 2007, at the following URL: http://www.netcaucus.org/books/privacy2001/pdf/cacmfinaldoc.pdf.

General consent: *Is it appropriate to capture the consumer's consent to a particular data collection, use, or disclosure as part of the umbrella privacy and terms of use policies? (See* ***CP2: Policy Notice to Consumers****.)*

– or –

Independent consent: *Are particular data collections, uses, or disclosures more appropriately handled by asking the consumer to indicate specific agreement separately from her general agreement to policies and terms of use?*

We note the following considerations about consent in the context of Consumer Access Services and PHRs:

- **Initial (i.e., general) consent is attached to a notice of privacy practices, and must be actively provided.** Because PHRs should be voluntary, there must be an initial process by which the consumer consents to initiate a PHR account. An opt-in mechanism is required to establish a relationship and the consumer's acquiescence to the general policies (e.g., privacy policy and terms of use) of the service. Such policies must be closely tied in to the registration process. *(See* ***CP2: Policy Notice to Consumers****.)*

- **However, initial opt-in consent is only one piece of a trust relationship.** The question is not merely: *"Did the consumer opt-in to the fine print?"* It is not sufficiently protective to consumers to rely solely on their agreement to policies as part of the initial registration process. As we discussed above, many consumers cannot make informed or meaningful choices based on policy notices that they often do not read, or cannot understand even if they do try to read them. A full complement of practices in this Common Framework must be addressed, not just a "blanket" consent mechanism during an initial registration process.
- **Further, many factors may influence a consumer's decisions.** This includes marketing, advertising claims, the brand, sponsor, and affiliations, and other "packaging." For example, if a Consumer Access Service advertises itself as "safe," or "private," or "secure," such claims can be presumed to help shape consumer expectations (more so, in many cases, than the notice of policies).
- **Choices should be meaningful.** All of the recommendations in ***CP2: Policy Notice to Consumers*** regarding clarity of language apply equally to consent mechanisms. Consumer Access Services must spell out clearly the consequences of each choice. Layered electronic notices, which afford general notice with links to more detailed information, may be a useful tool to provide the appropriate level of explanation for consumers to make meaningful, granular choices.
- **Consent should be easily amendable and revocable.** To the extent possible, consumers should have the ability to change their consent preferences at any time. It should be clearly explained whether such changes can apply retroactively to data copies already exchanged, or whether they apply only "going forward."
- **Appropriate consent is contextual.** For example, it's reasonable to expect that a PHR offered by a retail pharmacy chain would include a registered user's history of prescriptions filled through its stores. However, the consumer may not expect that the pharmacy would obtain non-medication information about the consumer from other entities without obtaining independent consent. Similarly, a consumer might expect a provider-based PHR that offers secure e-mail with clinicians to have those communications imported into the provider's EHR, but may not expect the publication of those communications in a journal article without specific consent.
- **Choices should be proportional.** The detail of a consumer's consent should be proportional to the sensitivity of the data, its uses, and disclosures, as well as the sophistication of the consumer.[4]

[4] Center for Democracy and Technology, Abrams, *Choice, Considering Consumer Privacy.*, March 2003, page 28. Accessed online on August 22, 2007, at the following URL: http://www.cdt.org/privacy/ccp/ccp.pdf.

- **Consent mechanisms should focus on reasonable expectations of an average consumer.** Consumer protection law provides a framework for determining whether consent for a given practice should be general or independent. A key question in consumer protection cases is whether, based on the company's overall actions and relationship with consumers, a reasonable person would be unaware of a practice in question.

Therefore, the general standard for independent consent centers on a reasonable consumer's expectations and is rooted in the principle that choices be proportional (i.e., the more sensitive, personally exposing, or inscrutable the activity, the more specific and discrete the opt-in). Based on the service's overall product and packaging (and not just what is listed in the general privacy policy and terms of use), reasonable consumers would expect to be asked specifically about a given activity, then an independent consent mechanism should be provided.[5]

Recommended Practice:

The general principle is that consumers should have meaningful choices spelled out in an understandable way. Consent mechanisms should set forth all collections, uses, and disclosures — including the reasons for such uses and disclosures. Consumer Access Services should obtain the consumer's agreement prior to any collection, use, or disclosure of personal data.

Data collections, uses, or disclosures of personal information that could be particularly sensitive or unexpected by a reasonable consumer, or any that pass the user's personally identifiable information to unaffiliated third parties[6], should be subject to additional consent and permissions (i.e., independent consent), which should be obtained from users in advance of the use or disclosure.

The tables below provide an example for how these principles could be put into practice for a variety of information that may be collected, used, or disclosed as part of a PHR or consumer data stream. We acknowledge that there is considerable burden, both for back-end systems and for consumers navigating a user interface, to highly granular permission sets.

Some consumers, with an established trust relationship with the service, may be comfortable forgoing the opportunity to give specific consent to specific uses and disclosures. Others may prefer to give specific consent to each type of requested use and disclosure. It may be appropriate in some cases to provide consumers with "default settings" and the ability to indicate whether or not they wish to exercise consent more or less granularly. Any default settings should bear in mind the "reasonable expectations" standard described above, and should clearly spell out the basic consequences of either accepting the default settings or changing them.

Because appropriate consent is contextual to a given relationship between a Consumer Access Service and the individual consumer, the table below is provided for **general guidance**. Whether an organization is covered by HIPAA, as well as what types of information it is sending to or receiving from a consumer application, will have some bearing on the appropriate approach to consumer consent. *(See **CP1: Policy Overview** for a discussion of HIPAA coverage.)*

[5] It is possible that general consent and independent consent options be provided during the same registration process. For example, during initial registration, an individual could sign on to the general terms of service, then be given the opportunity to opt-in to a particular type of data exchange. In practice, it can be a complex choice to determine whether a particular activity should be part of general consent or offered as an independent choice. At the time of initial registration, the consumer may not be able to understand or anticipate all of the future uses the PHR service may ultimately make of her data. In some cases, blanket consent to a set of generally described uses and disclosures may not be meaningful.

[6] We consider "affiliated" third parties to include those that, pursuant to a contract or agreement, collect, use, maintain, or disclose personally identifiable information on behalf of the PHR or Consumer Access Service (i.e., similar to a Business Associate under the HIPAA Privacy Rule). For example, a third party that maintains a server on behalf of the Consumer Access Service would be an affiliated third party. *(See **CP1: Policy Overview** for a discussion of HIPAA Business Associates.)* "Unaffiliated third parties" are third parties that collect, use, maintain or disclose such personally identifiable information for their own purposes or for the purpose of an entity other than the Consumer Access Service.

When a service or application seeks to ...	It should ...
Collect or use identifiable information[7] directly from consumers ...	• Provide adequate notice to consumers of practices used regarding personal data. (Notice should include what information the service collects, the purpose for which it is collected, whether subsequent transactions of the same type will be covered under the initial consent, how long the data will be stored, etc.) *(See **CP2: Policy Notice to Consumers**.)* • Obtain consent from the consumer prior to collection or use of such data. (Collections or uses that would be unexpected by a reasonable user should be subject to additional independent consent, which should be obtained from users in advance of the unexpected collection or use.)

When a service or application seeks to ...	It should ...
Collect or use indirectly identifying information[8] about consumers ...	• All of the above, plus: • Set forth in policy notices all collections of indirectly identifying information — and the purposes and uses of such collections. • Obtain consumer's independent consent prior to disclosing to unaffiliated third parties any information that can be directly or indirectly identifiable to an individual. *(See **CT4: Limitations on Identifying Information.**)*

[7] Examples of identifiable health information include:
- Contact information (e.g., name, address, e-mail address, phone number)
- Demographic information (e.g., date of birth, zip code, gender)
- Unique identifiers (e.g., social security number, health plan member ID)
- Health information (e.g., health status, lifestyle, habits, specific diagnoses, prognoses, test results, medications, medical services, health interests, health goals, family medical history, etc.)
- Financial information (e.g., credit card number and expiration date)
- Clinical and claims transactions

[8] We loosely define "indirectly identifying information" as data that is not individually identifiable at the point of collection, but that may used to uncover identity through analytic or linkage tools, or at least build a more complete profile of an individual. Examples of such data include:
- Clickstream, cookies, web beacons, and other similar methods
- IP addresses
- Search strings
- Data from other information brokers (e.g., household income, number of children, homeownership or rental status, magazine subscriptions)

When a service or application seeks to ...	It should ...
Collect or use identifiable information about consumers from unaffiliated third parties ...	• All of the above, plus: • Obtain the consumer's consent prior to collecting or using information about the consumer from unaffiliated third parties. • Use an independent consent mechanism for collections or uses of third-party data that are likely to be unexpected by a reasonable consumer.[9]
Disclose identifiable information to unaffiliated third parties ...	• All of the above, plus: • Employ notice and consent mechanisms that set forth all disclosures of personal information to third parties — including the purpose for, the uses of, and the policies governing such disclosures. • **NOT** disclose or expose to a third party information sufficient to identify a consumer, or to enable the third party to target the user directly, unless and until the consumer has provided independent consent to do so.[10]

When a service or application seeks to ...	It should ...
Collect, use, or disclose "de-identified" data ... *(See **CT4: Limitations on Identifying Information.**)*	• Provide adequate notice to consumers of the collections, uses, and disclosures of information designated as "de-identified data" — including the purposes for such collections, uses, and disclosures. Such notice should define what information is considered "de-identified," describe what processes are employed to make it so, and explain the potential risks of "re-identification." • Obtain general consent from the consumer prior to collection, use, or disclosure of such "de-identified data." • Prohibit, contractually and/or through other means, any unaffiliated third parties to which "de-identified data" is disclosed from attempting to "re-identify" the data by, among other things, combining it with other databases of information. *(See **CT4: Limitations on Identifying Information**.)*

[9] As an example, a reasonable consumer might expect her doctor's system to have gathered results from a third party laboratory service, or for her insurance company to know how much she paid as a co-pay. This type of information collected from third parties is less likely to be surprising to reasonable consumers. *(See **Appendix A of CT4: Limitations on Identifying Information** for a contrasting example of a reasonable consumer being surprised by data sharing among third parties.)*

[10] Legitimate exceptions may include complying with reasonable requests from law enforcement authorities. General policies for complying with law enforcement requests should be stated in the policy notice. *(See **CP2: Policy Notice to Consumers**.)*

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.*

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

CT1 CT2 CT3 CT4 CT5 CT6 CT7

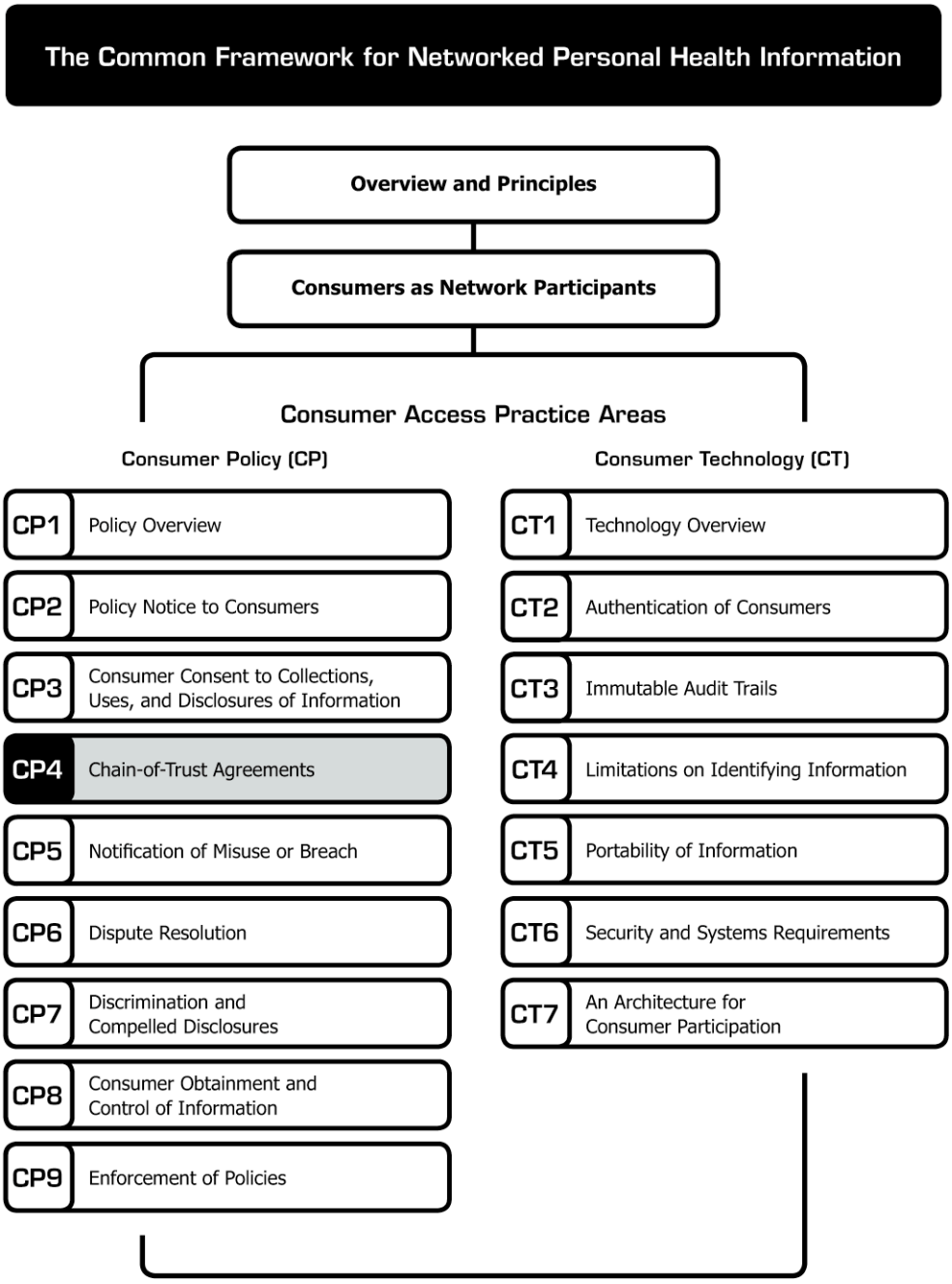
Chain-of-Trust Agreements

Chain-of-Trust Agreements

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:



Chain-of-Trust Agreements*

Purpose: For personal health information to flow in or out of a consumer-accessible application, it may pass among two or more organizations. Each participant in such "consumer data streams" may have its own legal and business interests to protect. However, consumers should be able to trust the entire chain of entities and business processes that handle their personal health data. Contracts are one mechanism to bind partners to specified privacy and security policies regarding confidential information they exchange or share.

Like other policy areas in this framework, chain-of-trust agreements are often necessary in certain relationships, but not by themselves sufficient to create a privacy-protective environment. In practice, such contracts have significant weaknesses, including their lack of transparency to consumers and their inconsistent enforcement. For one, breaches may not be discovered because organizations may not rigorously monitor the behavior of all of their business partners. Secondly, if an accusation of breach occurs, enforcement depends on one party engaging another party in a legal action, most likely under contract law. Organizations often seek to settle legal disputes out of court — or avoid litigation altogether.

Still, chain-of-trust agreements serve as important instruments in encouraging "good network citizenship." There are several possible relationships in which parties seek chain-of-trust agreements. HIPAA Business Associate agreements are one example. *(See **CP1: Policy Overview**.)*

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

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.

There is a problem with scaling this chain-of-trust model, however. It is unreasonable, for example, for each doctor's office to negotiate and sign a chain-of-trust agreement with every Consumer Access Service or networked PHR provider. Instead of each participant signing agreements with each other participant, it may be more practical if all participants agreed to a basic set of "network rules" — a set of common practices that each participant would sign and publicly commit to uphold. Although there are no such large-scale arrangements for Consumer Access Services or PHRs today, such models should be explored.

The HIPAA regulations permit consumers to request their personal health information directly from Covered Entities. Consumers may then store the information with any Consumer Access Service of their choice. In this case, the Consumer Access Service does not need a chain-of-trust agreement with the Covered Entity. The consent agreement(s) between the consumer and the Consumer Access Service should spell out the information-handling practices of the Consumer Access Service. (*See **CP4: Consumer Consent to Collections, Uses, and Disclosures of Information***.)

A Consumer Access Service may not be regulated under HIPAA, and it may have unregulated relationships with many different types of third parties. In such cases, chain-of-trust agreements between the Consumer Access Service and its third parties are a prudent mechanism to discourage unacceptable actions. Such agreements should prohibit activities that

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

are inconsistent with fair information practice principles, such as the surreptitious re-identification of de-identified data without the consumer's knowledge or consent. The recommended practice language below is primarily intended for this scenario (i.e., an uncovered Consumer Access Service's relationship with unrelated and unregulated third parties), but it may be helpful in other relationships as well.

Recommended Practice:

Consumer Access Services should contractually bind third parties with which they share or exchange personally identifiable, partially identifying, and de-identified data to:

- Prohibit unauthorized use and disclosure of such data.
- Protect the data in accordance with policies and authorizations agreed to by the consumer, when applicable.
- Prohibit unauthorized attempts to identify de-identified data by, among other things, combining it with other databases of information. (*See **CT4: Limitations on Identifying Information** for a discussion of personally identifiable, partially identifying, and "de-identified" data.*)
- Notify the Consumer Access Service if the third party is aware of a breach or misuse of information in a form that carries significant risk of compromising the security, confidentiality or integrity of personal information. (*See **CP5: Notification of Misuse or Breach**.*)

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.*

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

CT1 CT2 CT3 CT4 CT5 CT6 CT7

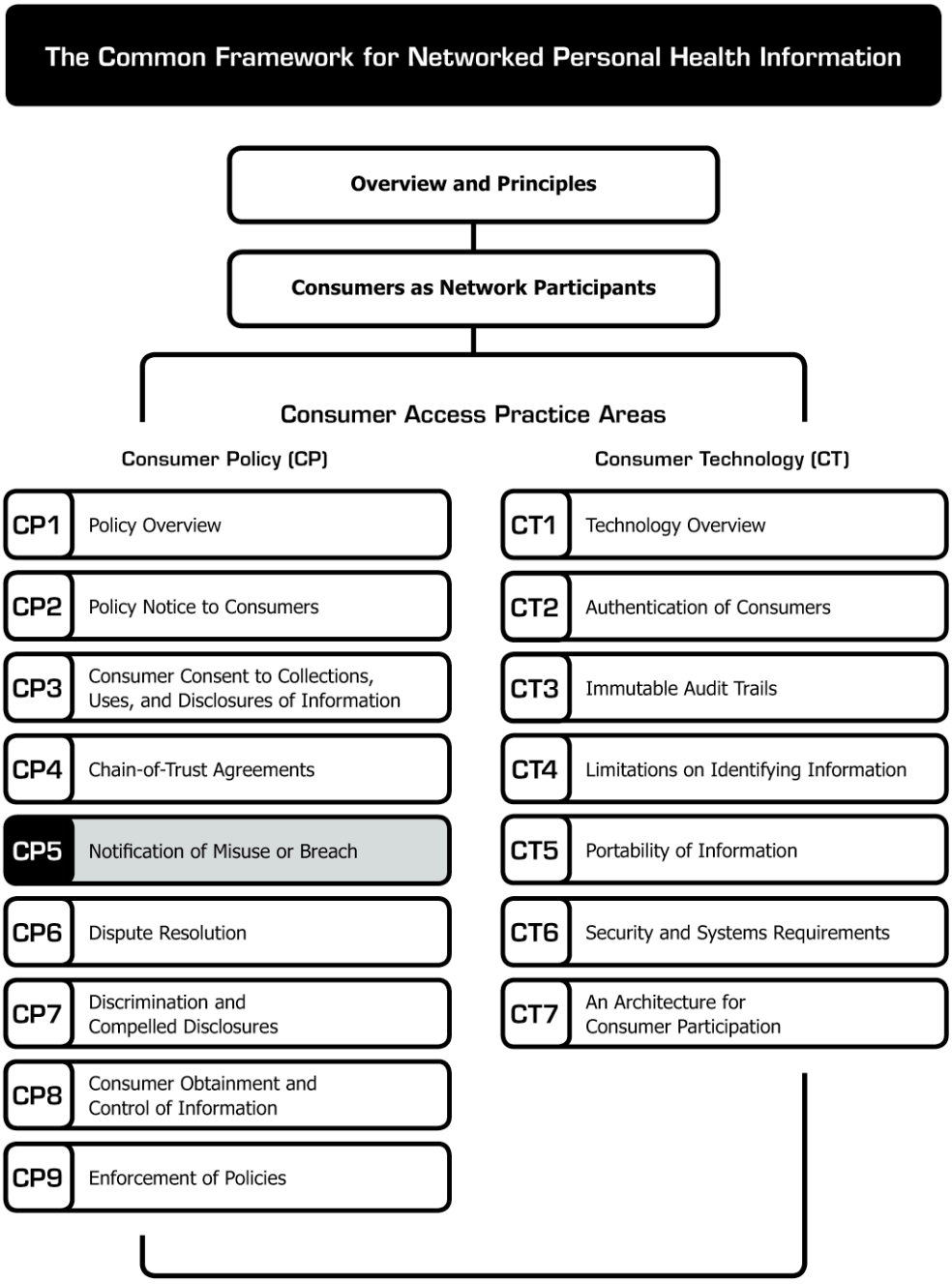
Notification of Misuse or Breach

Notification of Misuse or Breach

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:



Notification of Misuse or Breach*

Purpose: Secure and confidential data handling is a core responsibility for any Consumer Access Service. Part of this responsibility includes developing an advance plan on what the Consumer Access Service will do if something goes wrong. There have been many highly publicized inadvertent disclosures of sensitive personal data.

Our review of leading PHRs revealed a widespread lack of policy statements about responsibilities and actions that the company will take in the event of a breach or misuse of personal health information. (*See* ***Appendix A of CP2: Policy Notice to Consumers***.)

California is the leader among several states that have enacted laws requiring companies to notify affected consumers when sensitive, personally identifiable data are disclosed into unauthorized hands, but such requirements are not yet universal.[1] Notification regarding health data breaches is controversial and subject to debate. Open questions include, for instance, what constitutes a breach? What types of data are at issue? What constitutes notice?

We recommend that Consumer Access Services develop policies for breach or misuse of information. Such policies should be posted as part of the part of the publicly available notice of privacy and security policies. (*See* ***CP2: Policy Notice to Consumers***.) Notwithstanding the lack of guidance or industry acceptance, Consumer Access Service policies should notify users of what the service believes to be a significant breach, how it will notify users when a breach occurs, and what recourse the user has in the event of a breach.

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

5. Individual participation and control

7. Security safeguards and controls

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.

Recommended Practice:

A Consumer Access Service should notify individually any user whose personal information was, or is reasonably believed to have been, disclosed or acquired by an unauthorized person or party in a form that carries significant risk of compromising the security, confidentiality, or integrity of personal information.

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

[1] The Privacy Commissioner of Canada has a helpful resource, *Overview of American Breach Notification Laws*. February 22, 2007. Accessed online on August 22, 2007, at the following URL: http://www.privcom.gc.ca/parl/2007/sub_070222_06_e.asp.

The notification should be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Notification practices should be consistent with state-of-the-art security standards and should be "risk-based" — tailored to the potential risk to the consumer and the size, complexity, and nature of the Consumer Access Service's operations. A current "best practice" for notification is described by the California Department of Consumer Affairs.[2]

[2] California Department of Consumer Affairs, *Recommended Practices on Notice of Security Breach Involving Personal Information*. February 2007. Accessed online on September 6, 2007, at the following URL: http://www.privacyprotection.ca.gov/recommendations/secbreach.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.*

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

CT1 CT2 CT3 CT4 CT5 CT6 CT7

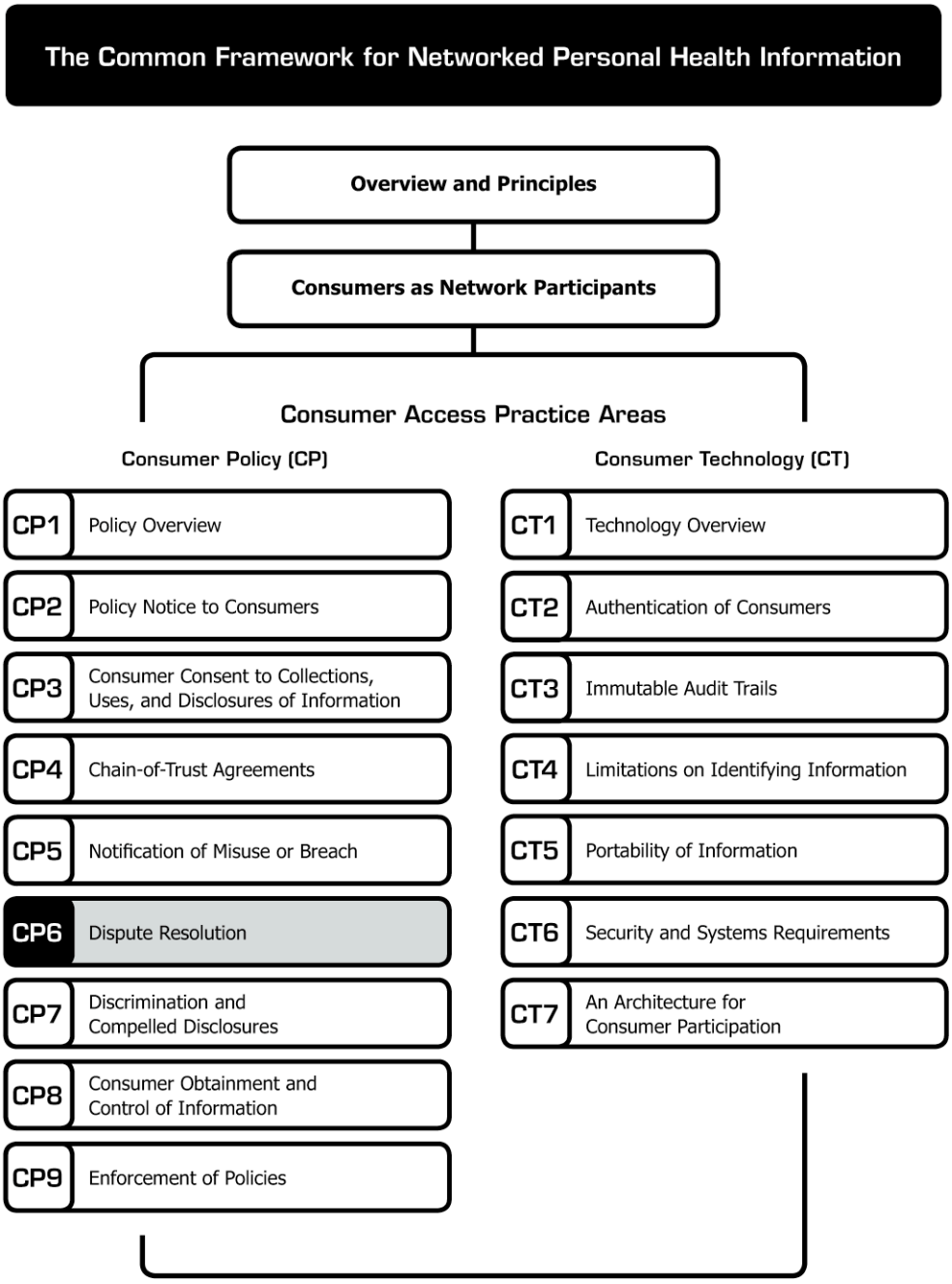
Dispute Resolution

Dispute Resolution

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:



Dispute Resolution*

Purpose: If they have concerns about their PHR or related services, consumers should have a transparent and easy-to-use process to resolve questions or disputes, such as:

- Misuse or breach of data. *(See **CP5: Notification of Misuse or Breach**.)*
- Disputes about privacy or data collection, handling, uses, or disclosures.
- Disputes claiming unfair or deceptive business practices.
- Data quality or matching errors.

Examples of trust-building mechanisms include but are not limited to the following:

- **Online negotiation:** PayPal's online Resolution Center[1] is an example of a service that enables buyers and sellers to negotiate and resolve disputes. If they fail, the case escalates to a PayPal claim, which the company investigates and resolves.
- **Ombudsman:** Used frequently in governments and industries such as journalism, an ombudsman is designed to be a neutral office charged with hearing and investigating complaints from the public.
- **Call centers:** In some organizations, existing call centers may serve to handle questions or disputes from consumers.

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

6. Data quality and integrity

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.

Consumers ideally will have a clear and logical pathway with effective options to raise and resolve disputes. At minimum, consumers should be provided with information to set realistic expectations about the service's practices for responding to complaints, as well as let consumers know where else they might effectively address their concerns. For example, if a consumer believes there is an error in data imported into her PHR from a Health Data Source, the consumer ideally will have easy access to information about how to contact that Health Data Source to request a correction, and at minimum should be able to easily identify who that Health Data Source is. *(See **CP8: Consumer Obtainment and Control of Information, Area 3: Requests to Amend or Dispute Entries.**)*

Recommended Practice:

PHRs and Consumer Access Services should set clear expectations for how consumers may address complaints. Ideally, PHRs and Consumer Access Services will provide clear and logical pathways for consumers to address and resolve complaints. Installing an ombudsman to accept and manage user disputes in a fair and convenient manner is one such mechanism.

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

[1] Accessed online on August 22, 2007, at the following URL: https://www.paypal.com/us/cgi-bin/webscr?cmd=xpt/CaseManagement/customerservice/EducationBuyerOverview [registration required].

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.*

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

CT1 CT2 CT3 CT4 CT5 CT6 CT7

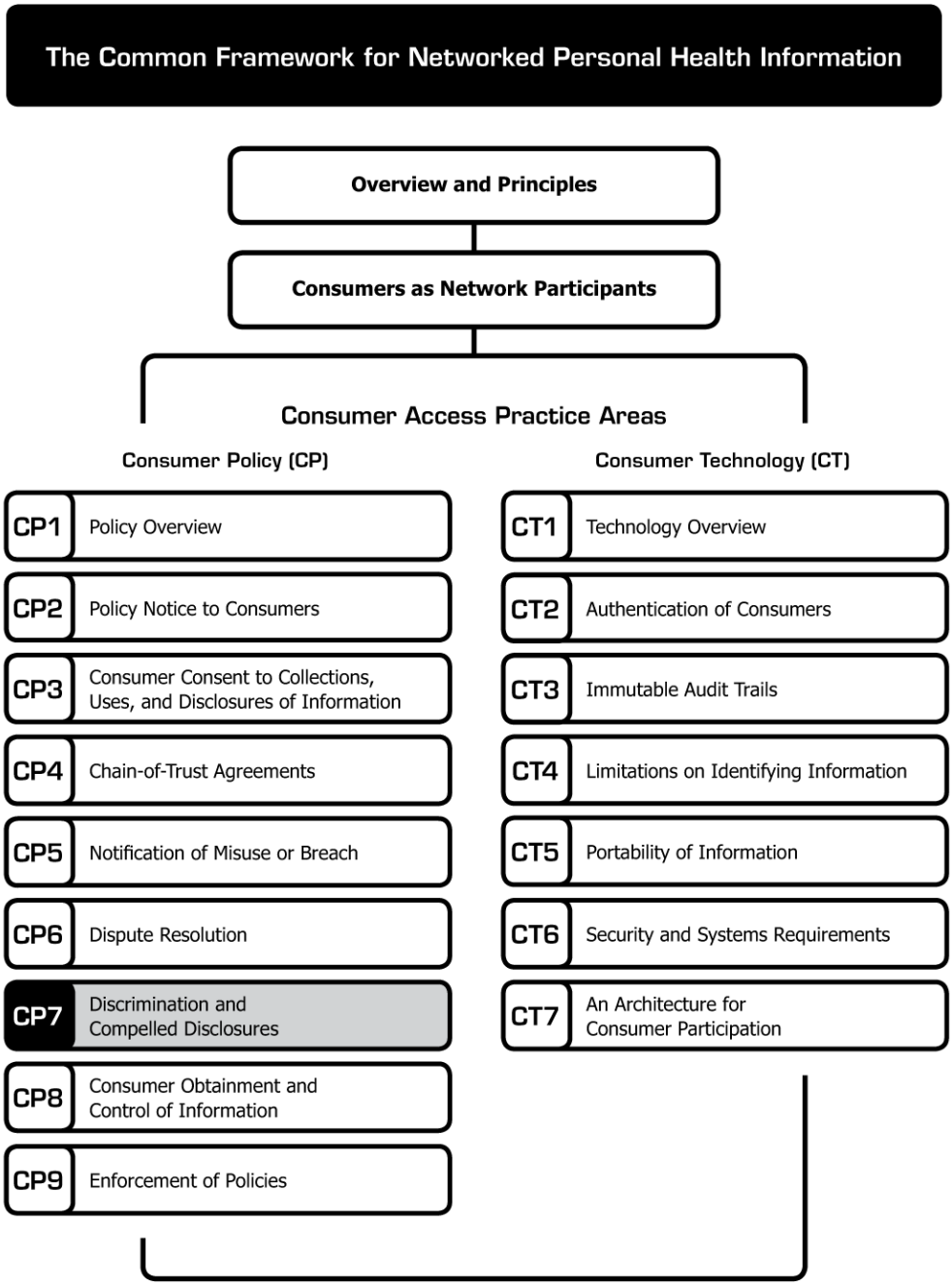
Discrimination and Compelled Disclosures

Discrimination and Compelled Disclosures

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:



Discrimination and Compelled Disclosures*

Purpose: Recent **Connecting for Health** public opinion research found that more than half of respondents were "very concerned" that employers or health plans would gain access to electronic information intended for PHRs.[1] Worry about possible employment or insurance discrimination likely drives these high numbers.

CT1: Technical Overview discusses "business data streams" and "consumer data streams." Business data streams consist of transactions of personal health information among business partners conducted without a consumer view or participation. For example, consumers generally don't see the transactions between their doctor's office and the insurance company, or between the insurance company and its data warehouse, etc. Consumer data streams involve transactions of information into or out of a consumer-accessible application, such as a PHR.

In addition to the enforcement of existing anti-discrimination laws, any organization acting as Consumer Access Service or PHR supplier should maintain a "firewall" between consumer data streams and business data streams to ensure that data captured or stored in consumer applications are not used as a basis for discrimination.

Our Work Group recommends that all network participants treat consumer data streams distinctly — with higher levels of protection than existing business streams of health data. This practice area recommends tough language to bar discrimination or "compelled disclosures" — such as when the consumer's authorization for release of data is required in order to obtain employment, benefits, or other services.

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

4. Use limitation

5. Individual participation and control

* "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.

Discrimination

It is important to recognize that consumer data streams and networked PHRs may lead to a commingling or at least co-existence of data from a variety of sources, including the consumer. It would threaten the consumer's trust in the entire network if the PHR were used as the source of information, no matter its origin, that affected an underwriting or employment decision. The **Connecting for Health** Common Framework policies for health information exchanges prohibit use of information for discriminatory purposes.[2] Similarly, employer groups have publicly stated that they will never access individually identifiable information generated and stored in the PHR services that they offer to their employees.

---

* **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.

[2] **Connecting for Health** Common Framework, *Model Privacy Policies and Procedures for Health Information Exchange*. June 2006, p. 10-11. Available online at: http://www.connectingforhealth.org/commonframework/docs/P2_Model_PrivPol.pdf.

Recommended Practice:

The preferred practice is to guarantee that none of the information made accessible to or from the consumer's application — that is, none of the consumer data stream — can ever be used to discriminate against consumers. In addition to complying with all anti-discrimination laws and regulations, all entities that access information in a consumer data stream should make public statements, and develop internal practices against using information in consumer data streams for purposes of discrimination. When appropriate, Consumer Access Services and PHRs should include anti-discrimination clauses in their contracts with partners. The best means of preventing information from being used for discrimination is to put in place strong policies and access control procedures.

It is noted that some organizations, particularly HIPAA-Covered Entities such as health plans and self-insured employers, collect personal health information to perform their business operations (i.e., as part of the business data stream) as well as offer Consumer Access Services. In addition to complying with all anti-discrimination laws and regulations, such organizations should use prudent practices such as implementing a "firewall" between consumer data streams and business data streams in order to prevent even the appearance of being able to use information in consumer data streams for purposes of discrimination.

Compelled Disclosures

According to the chair of the Subcommittee on Privacy and Confidentiality of the National Committee on Vital and Health Statistics: "Each year, as a condition of applying for employment, insurance, loans, and other programs, millions of individuals are compelled to sign authorizations permitting employers, insurers, banks, and others to access their personal health information for non-medical purposes. These authorizations are nominally voluntary; individuals are not required to sign them, but if they do not, they will not be considered for the particular job, insurance policy, loan, or benefit. In addition, for most of these authorizations, no limits are placed on the scope of the information disclosed or the duration of the authorization."[3]

Few laws or regulations place limits on such compelled disclosures. To date, most information released under such circumstances comes from what we call business data streams, e.g., from official medical records, etc.

If consumer data streams and PHRs are opened to such compelled authorizations, it will seriously undermine the public confidence in these new tools. If consumers fear that information in their networked PHR must be released to third parties considering their applications for employment, benefits, loans, etc., many will avoid health information services that might otherwise help them manage their health.

Recommended Practice:

Absent statutory protection from compelled disclosures, the emerging industry of Consumer Access Services should take a strong public and legal stand against third parties seeking to make their own access to consumer data streams and networked PHR information a condition of an individual's employment, benefits, or other services important to the well-being of individuals.

[3] Rothstein, Mark, June 2006 Letter to HHS Secretary Leavitt. Accessed online on October 9, 2007, at the following URL: http://www.ncvhs.hhs.gov/060622lt.htm. See also *Compelled Disclosure of Health Information: Protecting Against the Greatest Potential Threat to Privacy*. JAMA, Volume 295(24), 28 June 2006, p. 2882-2885.

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.*

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

CT1 CT2 CT3 CT4 CT5 CT6 CT7

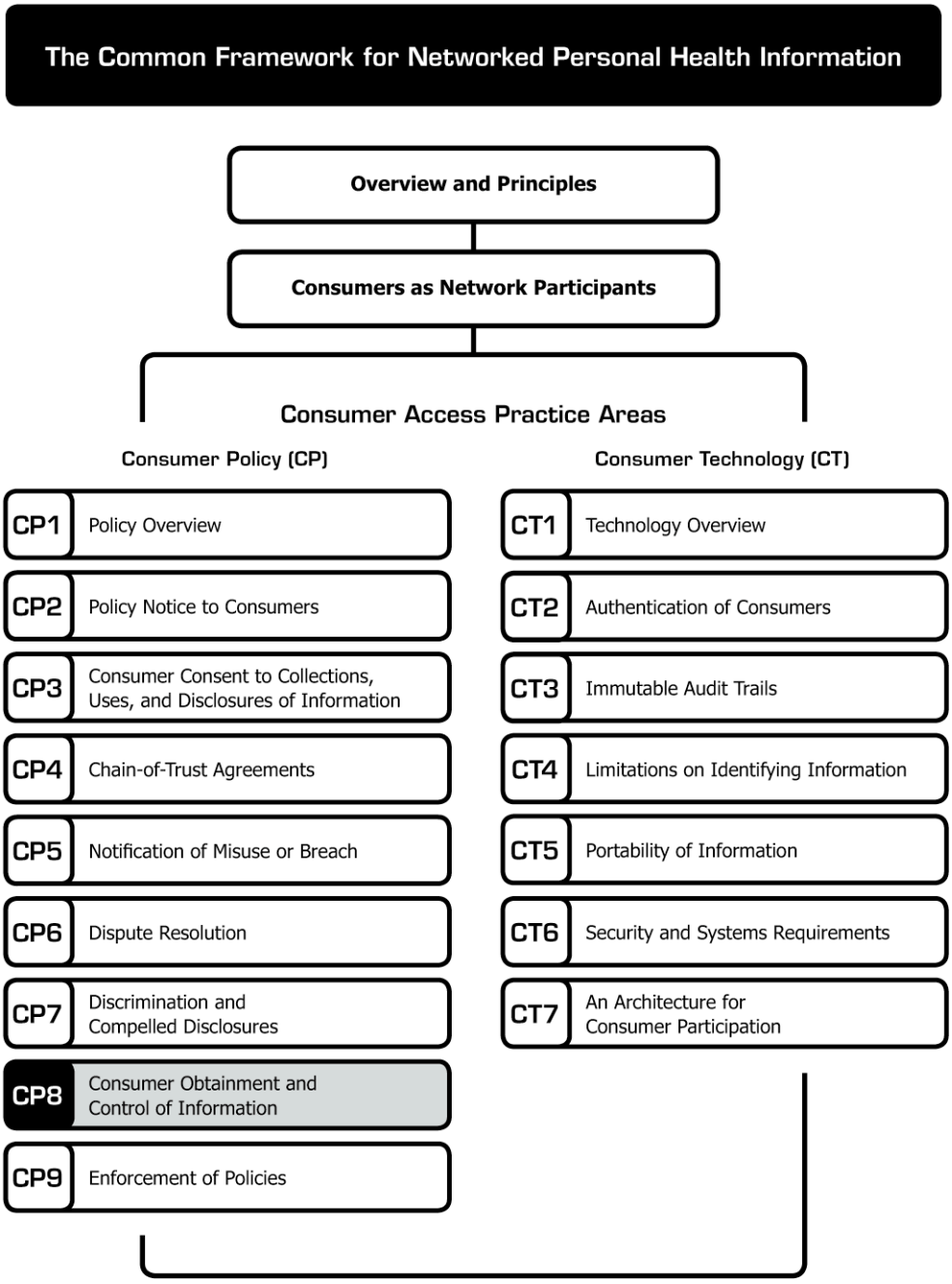
Consumer Obtainment and Control of Information

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.*

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

CT1 CT2 CT3 CT4 CT5 CT6 CT7

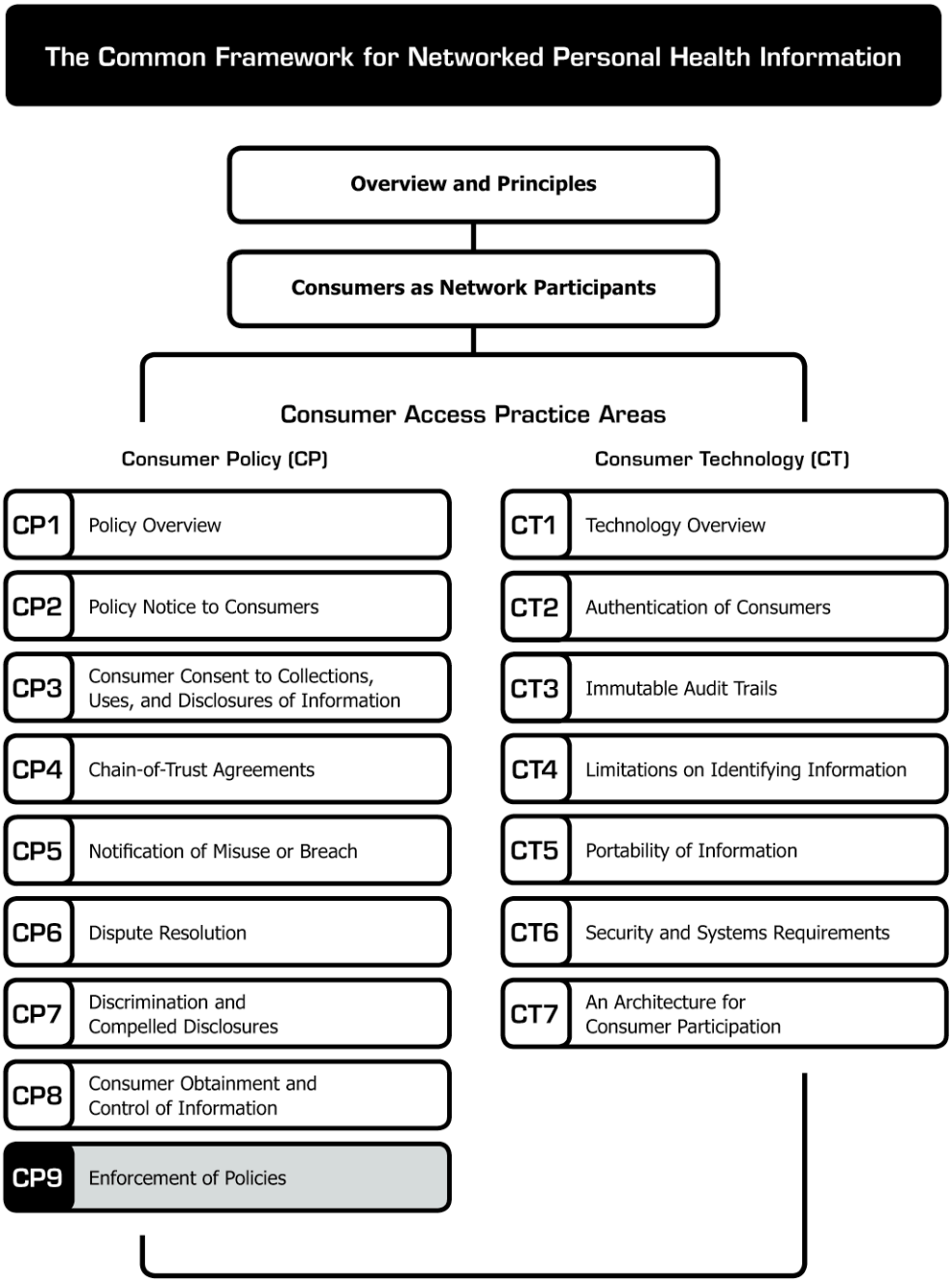
Enforcement of Policies

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*

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

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.

* **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.*

CP1 CP2 CP3 CP4 CP5 CP6 CP7 CP8 CP9

CT1 CT2 CT3 CT4 CT5 CT6 CT7

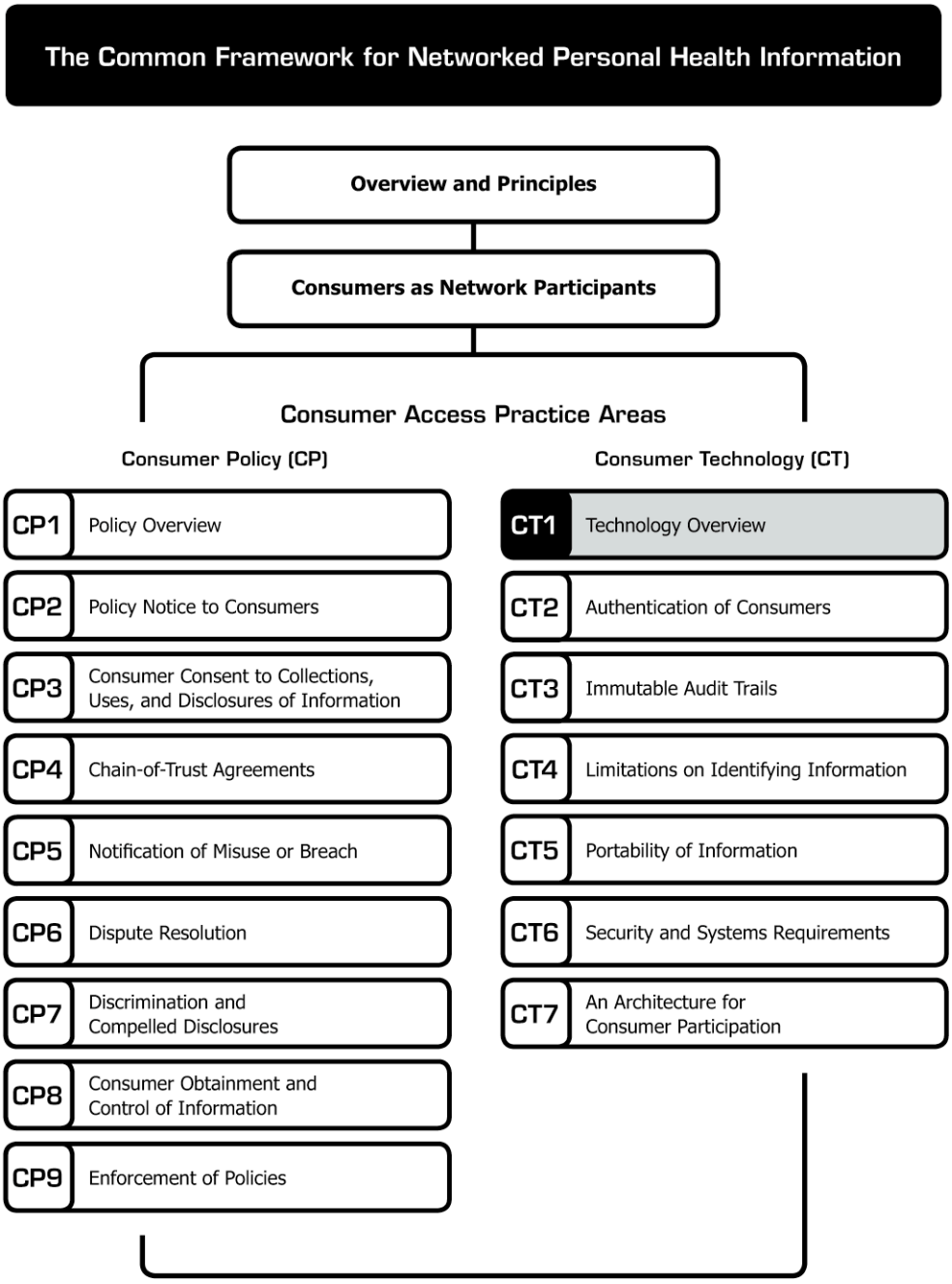
Technology Overview

Technology 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:



Technology Overview*

The health sector has long lagged other sectors in replacing paper recordkeeping with more efficient electronic information technology. Although health care reformers justifiably bemoan the long delays in modernizing health care, there is a large and growing store of digital health data. It includes electronic claims, e-prescribing and pharmacy dispensing scripts, images, labs, and information captured by clinicians in electronic health records (EHRs). Paralleling the slow expansion of digital health data used by providers and businesses, the last few years have also seen increased interest in PHRs as tools for consumers to better manage their health and health care.

Both trends are potentially beneficial. Both can help get the right information to the right people in a timely way. One way to look at the two trends is as separate categories of health data streams. We'll call them "**business data streams**" and "**consumer data streams**."

In both areas, but particularly in consumer data streams, no dominant suppliers have emerged. The role of federal or state oversight remains uncertain and contentious. Many social and political discussions are developing that reflect significant concerns about inappropriate uses of electronic personal health information, including the perceived risk to employment, insurance coverage, reputation, identity, or exposure to unauthorized marketing or solicitations. For these reasons, now is the critical time to examine the emerging digital data flows.

* **Connecting for Health** thanks Josh Lemieux, Markle Foundation, and David Lansky, PhD, for drafting this paper. A special thanks to Matt Kavanagh, independent contractor, for his diligent research and drafting of Appendix A.

In the Digital Age, 'Copies' Are What Matter

In an electronic environment, information can be rapidly copied and shared. A piece of data captured in one place may be forwarded to another, then another, and so on. Each time, the "sender" does not erase the data after passing it on. A copy is typically stored at each place. And each party that touches the data may add or modify information according to its business needs.

Because of this frequent copying and modifying, it is not useful or practical to discuss "ownership" of data in health care, in the sense that an owner of a paper file can allow use of the file without providing a copy. In the digital world, use of data proliferates copies as a side effect. And those copies, once made, must be retained by some recipients (e.g., medical professionals), by law. It is also not useful to apply old paradigms to protecting data such as locked file cabinets or creating lock boxes of electronic data. It is, however, critical to talk about proper custodianship of electronic personal health information copies — and under what authorizations and circumstances those copies may be shared.

The liquidity of health data copies creates both benefits (e.g., rapid retrieval, data analytics) and risks (e.g., personal privacy, errors).

Business Data Streams in Health Care

Throughout life, the typical consumer's health data is scattered among many health care providers, payers, clearinghouses, and other services (some of which are largely unknown to the public). Digital information flows through the health sector based on business requirements, typically with a complex series of handoffs stemming from business relationships. For example, **Appendix A** follows the data trail of a single drug prescription, the most common clinical transaction. Just to put the pills in the bottle, under the "simple" scenario, there are 10

different electronic copies of the information stored in various databases. The following are general observations about business data streams:

- There are multiple copies captured, cached, and/or warehoused at multiple locations. Electronically networked information can rarely be deleted without a trace.
- Businesses play various roles in the data stream. The personal health data copies create business value at various points. Just a few examples of copies creating value in aggregate or personal form (*See "Complex Case," in* ***Appendix A***.):
  - o Data aggregation companies sell de-identified prescription data to pharmaceutical companies, which use it in their sales representative meetings with physicians.
  - o Large claims clearinghouses sell data analytics services to payers or employers.
  - o Copies also are sent to preferred provider organizations for pricing, disease management companies for direct intervention, specialized services to detect fraud, etc.
- Different business entities participate at each handoff, with different business objectives and motivations. They may maintain different relationships with consumers, providers, payers, employers, etc. They each may have different internal policies and practices. And each may handle different subsets of the data, as information is continually filtered, scrubbed, augmented, etc., along the way.
- There are many potential points of vulnerability and exposure — in various repositories, archiving/backup, and hacking.
- The consumer has limited exposure to most business data streams. The typical consumer has no convenient way to know how her data will be stored or merged with other files, or re-identified. In short, it's very difficult for an individual to learn or understand very much about existing and emerging business health data streams.

Consumer Data Streams

We distinguish consumer data streams as the flow of personal health information into and out of consumer-accessible applications such as PHRs. There are increasing opportunities for consumers to participate in consumer data streams. Consumers are increasing their own contributions to new data streams by uploading health-related content about themselves to various Internet services. We are witnessing a proliferation of data streams through new services offering consumers the ability to obtain copies of information captured about them at various points along the business data stream. Large integrated delivery networks, employer groups, and payers have all launched plans to supply individuals with PHRs that can be pre-populated with personal health information from various sources.

There are several barriers, however, to such initiatives becoming interconnected on an open network. The current evolution of PHRs and Consumer Access Services reflects the fragmented health care sector. The current direction is that many of the more sophisticated PHR products will be based on specific business relationships with specific populations of consumers (e.g., integrated delivery networks, health plans, and employers offering PHRs to their respective members/employees). Many Health Data Sources are likely to favor their own PHRs, if they exist, over applications offered by third parties. New Consumer Access Services face a difficult task of negotiating contracts with the many Health Data Sources, each with its own business considerations and legal hurdles, in order to gain access to consumers' personal health data.

Secondly, data captured at any one point is often not valuable to consumers. It often needs to be combined with information from other sources and then given proper interpretation to be useful. Consumers will likely need new services to collect and add value to copies of their health data. (*See* ***Consumers as Network Participants***.)

A further privacy consideration is that the new consumer data streams will produce new generations of data copies and stores. There will be ever more opportunities for organizations to capture, combine, and share health information

about individuals. These new data sets include things like:

- IP addresses, cookies, and web beacons and similar technologies.
- Search keywords (which can be revealing about an individual's health concerns and often can be tied back to the individual).
- Information contributed by consumers (e.g., PHR data entries, patient diaries, consumer ratings services, online community posts).
- Information collected from health monitoring devices (e.g., blood pressure, blood glucose, etc.).
- Information collected by consumers (e.g., scanned documents and images, etc.).
- Genetic information.

(*See **Appendix A of CT4: Limitations on Identifying Information** for a discussion of how "partially identifying data" can be combined with other information to establish identity.*)

The emergence of consumer data streams poses a challenge to traditional health care institutions. Technology companies with powerful global brands operate within a vastly different business culture from health care organizations. They have different relationships with consumers, and separate legal and regulatory frameworks. Increased technology innovation and consumer participation will challenge traditional health care organizations as they seek the attention of the 21st Century patient/consumer, who is increasingly accustomed to Internet-based services in other sectors, such as finance or travel. Faced with increasing out-of-pocket health costs, as well as personal and societal needs for better health self-management, today's consumers need better tools as well as assurances that their information will be handled according to fair information practices.

Appendix A: Data Flow Scenarios

The following scenarios are designed to illustrate electronic data streams for the most common transaction in health care: a drug prescription. The first scenario describes a common and simplified set of transactions stemming from a small clinical practice. The second scenario adds sophistication and complexity, depicting transactions that are less common today (although they may become more common in the emerging electronic environment). The additional transactions increase potential value for many stakeholders, including the consumer, but also heighten the risk to privacy and security due to multiple round trips across data sources and copies being held by an increasing array of parties.

Note: The numeric sequence of "copies" below is designed to help the reader understand the parties that create and receive information related to a prescription transaction. A real-world chronology would be different than the sequence reflected here, as some transactions are batched with longer lag times than others.

Scenario 1 (SIMPLE)

Radhika Parekjhi, MD, works for a small practice that does not have an electronic health record (EHR) or e-prescribing application. The practice does, however, utilize practice management software for electronic claims submittal. Steve Jones, a pharmacist with ACME Pharmacy Chain, performs his work using a pharmacy information system that includes e-prescribing functionality.

- In follow-up to receiving abnormal blood test results at a health fair, Millie Robin makes an appointment to see Dr. Radhika Parekjhi.
- At the appointment, Dr. Parekjhi reviews Millie's current health status and health history (including her abnormal lab results), performs an exam, and orders additional tests. Based on this information, Dr. Parekjhi diagnoses a medical condition and decides to prescribe a new medication. (Millie's doctor's office stores this information, **copy I-1**, in the paper chart for Millie at the practice. The "I" designates a copy that includes "identifiable" data.)

Source of Data	Personal Data Transferred	Transfer Reason	Transaction Detail (Source --> **Recipient**)	**Recipient** Copy #	What Other Personal Data May the **Recipient** Have?
Millie (patient)	• Demographic/Contact • Insurance • Employment • Provider seen/referred • Biometric data (e.g., blood pressure) • Diagnoses/Problem list • Procedures • Medications • Allergies • Immunizations • Hospitalization history • Laboratory results • Other health history (e.g., family history of heart disease) • Lifestyle history (e.g., smoker) • Social history (e.g., married)	Information provided by Millie in the context of her appt. w/ Dr. Parekjhi	Millie --> Patient Registration (**Paper chart**) Millie --> Dr. Parekjhi and staff (**Paper chart**)	**I-1 (paper)**	• Visit history • Doctor progress notes • Other information specific to care received at this practice

- After reviewing Millie's current medications, problem list, and medication allergies, Dr. Parekjhi finds no contraindications or interactions and decides to prescribe medication "X" to treat Millie's newly diagnosed medical condition.
- Dr. Parekjhi writes a paper prescription for medication "X" and hands it to Millie.
- Dr. Parekjhi completes documentation for Millie's encounter, and the following day a coder employed by the practice electronically submits a claim to Millie's Health Plan (Payer) for payment. This information includes Millie's diagnosis, procedural and other personal health information.[1]

  o A Claims Clearinghouse entity receives the claim, processes it, and sends it to Millie's Payer in the Payer's required format. (Clearinghouse stores **copy I-2**.)

Source of Data	Personal Data Transferred	Transfer Reason	Transaction Detail (Source --> **Recipient**)	**Recipient** Copy #	What Other Personal Data May the **Recipient** Have?
Doctor office paper chart	• Demographic/Contact • Insurance • Health claim type (e.g., Workman's Comp) • Prescriber ID (e.g., DEA#) • Employment • Diagnoses • Procedures (including the CPT code that contains the prescribed medication)	Health claim submitted to Payer	Doctor's office --> **Claims Clearninghouse**	**I-2**	Other claims submitted to same Clearinghouse

  o The Clearinghouse sells aggregated de-identified data to research companies as part of its revenue model. (A Health Care Market Research Company stores de-identified **copy DI-1.** "DI" stands for data that has been "de-identified".)

Source of Data	Personal Data Transferred	Transfer Reason	Transaction Detail (Source --> **Recipient**)	**Recipient** Copy #	What Other Personal Data May the **Recipient** Have?
Clearinghouse	De-identified data	Generate revenue	Claims Clearninghouse -> **Health Care Market Research Company**	**DI-1**	n/a

[1] Example of a Payer claim form: https://www.lifewisewa.com/lwwa/groups/public/documents/pdfs/002636.pdf.

- Millie's Payer receives the claim from the Clearinghouse and adjudicates the claim. (Payer stores **copy I-3**.)

Source of Data	Personal Data Transferred	Transfer Reason	Transaction Detail (Source --> **Recipient**)	**Recipient** Copy #	What Other Personal Data May the **Recipient** Have?
Clearinghouse	• Demographic/Contact • Insurance • Health claim type (e.g., Workman's Comp) • Prescriber ID (e.g., DEA#) • Employment • Diagnoses • Procedures	Claim processing completed; ready for adjudication	Claims Clearinghouse --> **Payer**	**I-3**	Other claims for Millie submitted to this same Payer

  o Millie's Payer sends a de-identified copy of Millie's data to a third-party organization for data analysis. This third-party stores **copy DI-2**.

Source of Data	Personal Data Transferred	Transfer Reason	Transaction Detail (Source --> **Recipient**)	**Recipient** Copy #	What Other Personal Data May the **Recipient** Have?
Payer	De-identified data	Analysis on quality and effectiveness	Payer --> **Data Analytics Company**	**DI-2**	n/a

- Millie arrives at her Pharmacy and hands the paper prescription to a pharmacist assistant. As required by protocol, the assistant confirms Millie's information and collects additional information required to process/fulfill the prescription. (Millie's Pharmacy stores the information in its system, **copy I-4**.)

Source of Data	Personal Data Transferred	Transfer Reason	Transaction Detail (Source --> **Recipient**)	**Recipient** Copy #	What Other Personal Data May the **Recipient** Have?
Millie's prescription	• Demographic/Contact • Insurance • Prescriber ID • Medication prescribed (medication "x")	Millie presents in-person to fill her new prescription	Millie's paper prescription--> **Millie's Pharmacy**	**I-4**	Other prescriptions filled at this Pharmacy (and chain if applicable)

- The pharmacist assistant who receives Millie's prescription makes a "Formulary and Benefits and Drug Utilization Review" request via the Pharmacy's information system to Millie's Pharmacy Benefits Manager (PBM) via a pharmacy claims processing network or via a direct connection between the Pharmacy and the PBM. (Millie's PBM stores **copy I-5**.)

Source of Data	Personal Data Transferred	Transfer Reason	Transaction Detail (Source --> **Recipient**)	**Recipient** Copy #	What Other Personal Data May the **Recipient** Have?
Pharmacy	• Demographic/Contact • Medication prescribed (medication "x")	Formulary and Benefit and Drug Utilization Review (REQUEST)	Pharmacy --> **Millie's PBM** (via claims processing network)	**I-5**	Claims-based Rx history data, specific to the PBM

- Millie's PBM sends the requesting Pharmacy a response message which includes a confirmation of Millie's medication benefits eligibility (i.e., whether the PBM accepts or rejects the claim), Millie's co-pay for medication "X," and a message indicating that no medication interactions were found based on Millie's medication history (as known by this PBM). Millie's Pharmacy stores **copy I-6.**

Source of Data	Personal Data Transferred	Transfer Reason	Transaction Detail (Source --> **Recipient**)	**Recipient** Copy #	What Other Personal Data May the **Recipient** Have?
Millie's PBM	• Demographic/Contact • Insurance • Interaction alert(s)	Formulary and Benefit and Drug Utilization Review (RESPONSE)	Millie's PBM (via claims processing network) --> **Pharmacy**	**I-6**	Other prescriptions filled at this Pharmacy (and chain if applicable)

- Pharmacist Steve Jones fills the prescription and Millie pays the co-pay.
  - o Because the Pharmacy is part of a larger chain, a copy of Millie's prescription transaction is sent to the Pharmacy's Central Data Warehouse. (The Pharmacy's central data warehouse stores **copy I-7**.)

Source of Data	Personal Data Transferred	Transfer Reason	Transaction Detail (Source --> **Recipient**)	**Recipient** Copy #	What Other Personal Data May the **Recipient** Have?
Pharmacy	• Demographic/Contact • Insurance • Prescriber ID (e.g., NPI) • Medication(s) prescribed and/or dispensed	Transfer of information to Pharmacy's data warehouse	Pharmacy --> **Pharmacy's Central Data Warehouse**	**I-7**	Other prescriptions previously filled by this Pharmacy chain

- The Pharmacy submits a claim to Millie's PBM for payment. (Millie's PBM stores **copy I-8**.)

Source of Data	Personal Data Transferred	Transfer Reason	Transaction Detail (Source --> **Recipient**)	**Recipient** Copy #	What Other Personal Data May the **Recipient** Have?
Pharmacy	• Demographic/Contact • Insurance • Prescriber ID (e.g., NPI) • Medication(s) prescribed and/or dispensed • Claim information	Pharmacy requests payment for Millie's medication	Pharmacy --> **Millie's PBM**	**I-8**	Other claims for Millie submitted to this PBM for adjudication

- Millie's PBM adjudicates the claim and sends it to Millie's Payer for payment. (Millie's Payer stores **copy I-9**.)

Source of Data	Personal Data Transferred	Transfer Reason	Transaction Detail (Source --> **Recipient**)	**Recipient** Copy #	What Other Personal Data May the **Recipient** Have?
Pharmacy	• Demographic/Contact • Adjudicated claim	Payment of medication claim	Millie's PBM --> **Millie's Payer**	**I-9**	Other claims for Millie submitted to this Payer

- Millie's Payer sends Millie's adjudicated claims data ready for payment to a Third Party Administrator (TPA) that pays each claim (the doctor's visit and Pharmacy claim) and sends Millie an Explanation of Benefits (EOB) detailing financial components of her visit with Dr. Parekjhi, including the amount billed, amount eligible for payment, insurance benefit paid or applied to deductible, and Millie's expected remaining balance due. (The TPA stores **copy I-10**.)

Source of Data	Personal Data Transferred	Transfer Reason	Transaction Detail (Source --> **Recipient**)	**Recipient** Copy #	What Other Personal Data May the **Recipient** Have?
Payer	• Demographic/Contact • Millie's adjudicated claims data	To enable the TPA to pay Millie's claim and send Millie an EOB	Health Plan (Payer) --> **Third Party Administrator -> Millie**	**I-10**	Other adjudicated data about Millie received by this TPA

- Millie's PBM may be allowed to de-identify the transaction and send this de-identified data to a Pharmaceutical Manufacturer and/or sell it to a Pharmaceutical Market Intelligence Company. (The Pharmaceutical Manufacturer and Pharmaceutical Market Research Company each store a copy of Millie's de-identified data, **copies DI-3**.)

Source of Data	Personal Data Transferred	Transfer Reason	Transaction Detail (Source --> **Recipient**)	**Recipient** Copy #	What Other Personal Data May the **Recipient** Have?
PBM	De-identified data	Generate revenue or fulfill contractual obligations	PBM --> **Pharmaceutical Market Research Company**	**DI-3**	n/a

Scenario 2 (COMPLEX)

Jennifer Smith, MD, works for a hospital medical group that uses practice management software and an electronic health record (EHR) that includes e-prescribing and electronic claims submittal functionality; Steve Jones, a pharmacist with ACME Pharmacy Chain, performs his work using a pharmacy information system that includes e-prescribing functionality.

- In follow-up to receiving abnormal blood test results at a health fair, Millie Robin makes an appointment to see Dr. Smith.
- At the appointment, Dr. Smith reviews Millie's current health status and health history (including her abnormal test results), performs an exam, and orders additional tests. Based on this information, Dr. Smith diagnoses a medical condition and decides to prescribe a new medication. (The Hospital's EHR stores a copy of this information, **copy I-1**. The "I" designates "identifiable data.")

Source of Data	Personal Data Transferred	Transfer Reason	Transaction Detail (Source --> **Recipient**)	**Recipient** Copy #	What Other Personal Data May the **Recipient** Have?
Millie (patient)	• Demographic/Contact • Insurance • Employment • Provider seen/referred • Biometric data (e.g., blood pressure) • Diagnoses/ Problem list • Procedures • Medications • Allergies • Immunizations • Hospitalization history • Laboratory results • Other health history (e.g., family history of heart disease) • Lifestyle history (e.g., smoker) • Social history (e.g., married)	Millie's appt. w/ Dr. Smith	Millie --> Patient Registration/ Scheduling (**Hospital PMS/EHR**) Millie --> Dr. Smith and staff (**Hospital EHR**)	**I-1**	• Doctor progress notes • Visit history • Other information specific to care received at Hospital

- Before proceeding, Dr. Smith uses her e-prescribing tool to make an Rx History Request.[2] This request is for the past 120 days of Millie's retail prescription history and includes Millie's Name, DOB, and Gender. This information is submitted electronically and routed through SureScripts Pharmacy Health Information Exchange (PHIE). (SureScripts and Hospital's EHR store **copies I-2** and **I-3**, respectively.) (Note that alternatively, Dr. Smith's e-prescribing tool may allow her to request a Claims Medication History from Millie's PBM to receive prescription history from all pharmacies, including mail-order, for which Millie used her medication benefits. However, the specifics of this alternative scenario are not covered here.)

Source of Data	Personal Data Transferred	Transfer Reason	Transaction Detail (Source --> **Recipient**)	**Recipient** Copy #	What Other Personal Data May the **Recipient** Have?
Hospital EHR	• Demographic/Contact • Prescriber ID (e.g., NPI)	Retrieve last 120 days of Rx history (REQUEST)	Hospital EHR --> SureScripts --> Pharmacy networks --> **SureScripts**	**I-2**	Retail-based Rx history data older than 120 days
SureScripts	• Demographic/Contact • Medication history	Retrieve last 120 days of Rx history (RESPONSE)	SureScripts --> **Hospital EHR**	**I-3**	n/a

- After reviewing/confirming Millie's updated retail medication history, problem list, and medication allergies and finding no potential contraindications or interactions, Dr. Smith informs Mille that she would like to prescribe medication "X" to treat her medical condition.
- Because Millie expresses concern about the possibility of high out-of-pocket costs, Dr. Smith uses her e-prescribing tool to make a Formulary and Benefits Information[3] request to determine whether medication "X" is on Millie's pharmacy benefits formulary. (Note that more commonly in offices with e-prescribing and scheduling software, this type of transaction is handled automatically via an interface between the two systems.)

[2] Personal data transferred based on the SureScripts Rx History service: http://www.ncvhs.hhs.gov/040330p2.pdf.

[3] Personal data transferred based on RxHub's PRN service: http://www.rxhub.net/pdf/rxhub_prn.pdf.

o Millie's First/Last Name, DOB, Gender, Zip Code, and medication X are electronically transmitted to RxHub (a "switch of switches" for major pharmacy benefit managers, or PBMs) to uniquely identify Millie in RxHub's Master Patient Index prior to RxHub routing the request to Millie's current Pharmacy Benefits Payer/PBM. (RxHub does not store a copy of data received/sent.) Millie's PBM receives the request (and stores copy **I-4**), and routes a response back through RxHub to Dr. Smith's EHR via the e-prescribing application. The response message indicates that Millie is eligible for prescription drug coverage and that the medication is on formulary but requires "prior-authorization."

Source of Data	Personal Data Transferred	Transfer Reason	Transaction Detail (Source --> **Recipient**)	**Recipient** Copy #	What Other Personal Data May the **Recipient** Have?
Hospital EHR	• Demographic/Contact • Medication prescribed (medication "x")	Benefits Eligibility and Formulary Request (REQUEST)	Hospital EHR --> **Millie's PBM**	**I-4**	Claims-based Rx history data, specific to the PBM
Millie's PBM	• Demographic/Contact • Insurance • Prior-authorization status	Benefits Eligibility and Formulary Request (RESPONSE)	Millie's PBM --> **Hospital EHR**	Not stored	

- Millie is satisfied with the formulary information (and expected out-of-pocket costs), and asks Dr. Smith to have the prescription sent to her local Pharmacy.
- Because Millie's medication requires prior-authorization (a medical necessity review of clinical data submitted by the prescribing physician and available prescription drug history against pre-established clinical criteria), Dr. Smith must fill out additional diagnosis and medication history for Millie and fax a completed prior-authorization request to Millie's PBM with an expected one-business day turnaround time to receive request approval.[4] (Millie's PBM stores **copy I-5**.)

Source of Data	Personal Data Transferred	Transfer Reason	Transaction Detail (Source --> **Recipient**)	**Recipient** Copy #	What Other Personal Data May the **Recipient** Have?
Hospital EMR	• Demographic/Contact • Insurance • Prescriber ID (e.g., NPI) • Diagnoses/Problem list • Medication(s) prescribed	Prior-Authorization for medication is required	Hospital --> **Millie's PBM**	**I-5 (paper fax)**	Claims-based Rx history data, specific to the PBM Additional health data, see **I-13**

[4] Example of a PBM Prior-Authorization form for Provigil: https://www.pharmacare.com/shared/pdf/PAForms/Provigil_Prior_Auth_Form.pdf.

- Confident that Millie's PBM will approve the new medication, Dr. Smith uses the e-prescribing application's pharmacy directory to find Millie's Pharmacy and send the prescription electronically. This request/response is sent via SureScripts PHIE.[5] (SureScripts stores **copy I-6**.)

Source of Data	Personal Data Transferred	Transfer Reason	Transaction Detail (Source --> **Recipient**)	**Recipient** Copy #	What Other Personal Data May the **Recipient** Have?
Hospital EHR	• Demographic/Contact • Pharmacy # • Prescriber ID (e.g., NPI) • Medication(s) prescribed	e-Prescription, step 1 of 2	Hospital EMR --> **SureScripts**	**I-6**	Retail-based Rx history data

- Dr. Smith completes documentation for Millie's encounter, and a claim is sent to Millie's plan sponsor (Payer) for payment. This information includes diagnosis, procedural, and other personal health information[6] about Millie.
  - o A Claims Clearinghouse receives the claim, processes it, and sends it along to Millie's Payer in the required format. (Clearinghouse stores **copy I-7**.)

Source of Data	Personal Data Transferred	Transfer Reason	Transaction Detail (Source --> **Recipient**)	**Recipient** Copy #	What Other Personal Data May the **Recipient** Have?
Hospital EMR	• Demographic/Contact • Insurance • Health claim type (e.g., Workman's Comp) Demographic/Contact • Prescriber ID (e.g., DEA#) • Employment • Social history (e.g, married) • Diagnoses • Procedures	Health insurance claim submitted to Payer	Hospital EMR --> **Claims Clearinghouse**	**I-7**	Other claims submitted to same Clearinghouse

[5] Personal data transferred based on the SureScripts e-Prescribing service: http://www.ncvhs.hhs.gov/040330p2.pdf.

[6] Example of a payer claim form: http://www.lifewisewa.com/lwwa/groups/public/documents/pdfs/002636.pdf.

o The Clearinghouse sells aggregated de-identified data to health care market research companies for profit. (Health Care Market Research Company stores de-identified **copy DI-1.** DI indicates de-identified information.)

Source of Data	Personal Data Transferred	Transfer Reason	Transaction Detail (Source --> **Recipient**)	**Recipient** Copy #	What Other Personal Data May the **Recipient** Have?
Clearinghouse	De-identified data	Generate revenue	Claims Clearinghouse --> **Health Care Market Research Company**	**DI-1**	n/a

o If the Hospital that employs Dr. Smith has rights to Millie's Rx data, the Hospital may de-identify it and sell it to a health care market intelligence company. (The Health Care Market Research Company stores de-identified **copy DI-2**.)

Source of Data	Personal Data Transferred	Transfer Reason	Transaction Detail (Source --> **Recipient**)	**Recipient** Copy #	What Other Personal Data May the **Recipient** Have?
Hospital EHR	De-identified data	Generate revenue	Hospital --> **Health Care Market Research Company**	**DI-2**	n/a

The Payer receives the claim from the Clearinghouse, adjudicates it, and pays the Hospital. (Payer stores **copy I-8**.)

Source of Data	Personal Data Transferred	Transfer Reason	Transaction Detail (Source --> **Recipient**)	**Recipient** Copy #	What Other Personal Data May the **Recipient** Have?
Clearinghouse	• Demographic/Contact • Insurance • Health claim type (e.g., Workman's Comp) Demographic/Contact • Prescriber ID (e.g., DEA#) • Employment • Social history (e.g, married) • Diagnoses • Procedures	Clearinghouse requests reimbursement from Payer	Claims Clearinghouse --> **Payer**	**I-8**	Other claims for Millie while she has received health insurance from this Payer

- Millie's Payer sends de-identified data about Millie to a third-party organization for data analysis. (Data Analytics Company stores copy **DI-3**.)

Source of Data	Personal Data Transferred	Transfer Reason	Transaction Detail (Source --> **Recipient**)	**Recipient** Copy #	What Other Personal Data May the **Recipient** Have?
Payer	De-identified data	Analysis on quality and effectiveness	Payer --> **Data Analytics Company**	**DI-3**	n/a

- Millie's Pharmacy's information system receives the prescription request via SureScripts.[7] (Millie's Pharmacy stores **copy I-9**.)

Source of Data	Personal Data Transferred	Transfer Reason	Transaction Detail (Source --> **Recipient**)	**Recipient** Copy #	What Other Personal Data May the **Recipient** Have?
SureScripts	• Demographic/Contact • Prescriber ID • Medication(s) prescribed	e-Prescription, step 2 of 2	SureScripts --> **Millie's Pharmacy**	**I-9**	Other prescriptions filled at this Pharmacy (and chain if applicable), and any MTM program data

  - Following protocol, the pharmacist assistant who receives Millie's prescription makes a "Formulary and Benefit and Drug Utilization Review" request via a pharmacy claims processing network or via a direct connection between the Pharmacy and the PBM. (Millie's PBM stores **copy I.10**.)

Source of Data	Personal Data Transferred	Transfer Reason	Transaction Detail (Source --> **Recipient**)	**Recipient** Copy #	What Other Personal Data May the **Recipient** Have?
Pharmacy	• Demographic/Contact • Medication(s) prescribed	Formulary and Benefit and Drug Utilization Review (REQUEST)	Pharmacy --> **Millie PBM** (via a claims processing network)	**I-10**	Claims-based Rx history data, specific to the PBM

[7] Personal data transferred based on the SureScripts e-Prescribing Service: http://www.ncvhs.hhs.gov/040330p2.pdf.

- Millie's PBM sends the Pharmacy a confirmation of Millie's medication benefits eligibility (i.e., whether the PBM accepts or rejects the claim) along with Millie's co-pay, a notice that prior-authorization has been granted, and a message indicating that no medication interactions were found based on Millie's medication history (as known by her current PBM). Millie's Pharmacy stores **copy I-11**.

Source of Data	Personal Data Transferred	Transfer Reason	Transaction Detail (Source --> **Recipient**)	**Recipient** Copy #	What Other Personal Data May the **Recipient** Have?
Millie PBM	• Demographic/Contact • Insurance • Interaction alert(s) • Prior-authorization status	Formulary and Benefit and Drug Utilization Review (RESPONSE)	Millie PBM (a claims processing network) --> **Pharmacy**	**I-11**	Other prescriptions filled at this Pharmacy (and chain if applicable), and any MTM program data

- Pharmacist Jones fills the prescription and Millie arrives to pick it up/pay for it.
  - Because the Pharmacy is part of a larger chain, a copy of Millie's prescription transaction is sent to the Pharmacy's Central Data Warehouse. (Millie's Pharmacy Demographic/ContactCentral Data Warehouse stores **copy I-12**.)

Source of Data	Personal Data Transferred	Transfer Reason	Transaction Detail (Source --> **Recipient**)	**Recipient** Copy #	What Other Personal Data May the **Recipient** Have?
Pharmacy	• Demographic/Contact • Insurance • Prescriber ID (e.g., NPI) • Medication(s) prescribed and/or dispensed	Transfer of information to Pharmacy's data warehouse	Pharmacy --> **Pharmacy's Central Data Warehouse**	**I-12**	Other prescriptions previously filled by this Pharmacy chain

  - If the prescribed medication is a schedule II controlled substance, the Pharmacy is typically required to send the state a copy of Millie's Rx data to be fed into a government system aimed at identifying and curbing prescription drug abuse. (State/Fed Rx Data Warehouse stores copy **I-13**.)

Source of Data	Personal Data Transferred	Transfer Reason	Transaction Detail (Source --> **Recipient**)	**Recipient** Copy #	What Other Personal Data May the **Recipient** Have?
Pharmacy	• Demographic/Contact • Prescriber ID • Medication(s) dispensed	Rx (controlled-substance) patient registry	Pharmacy --> **State/Fed Rx Data Warehouse**	**I-13**	Other Rx (controlled-substance only) information about Millie

- Via an e-Alert, the Pharmacy Information System informs Pharmacist Jones that Millie qualifies for a Medication Therapy Management (MTM) program offered by her PBM. As part of the Pharmacist-patient dialog, Pharmacist Jones informs Millie of her eligibility, receives her authorization to participate, and then collects additional PHI before educating her about medication use optimization/adherence and how to reduce the risk of adverse drug events through avoidance of certain drug and food interactions.
  - o Pharmacist Jones submits an electronic claim to Millie's PBM for reimbursement for MTM services he provided.[8] (Millie's PBM stores **copy I-14**.)

Source of Data	Personal Data Transferred	Transfer Reason	Transaction Detail (Source --> **Recipient**)	**Recipient** Copy #	What Other Personal Data May the **Recipient** Have?
Pharmacy	• Demographic/Contact • Insurance • Medication(s) dispensed • MTM procedures (CPT)	Receive payment for MTM services provided to Millie	Pharmacy--> **Millie's PBM**	**I-14**	Claims-based Rx history data, specific to the PBM

- The Pharmacy submits a claim to Millie's PBM for payment. (Millie's PBM stores copy **I-15**.)

Source of Data	Personal Data Transferred	Transfer Reason	Transaction Detail (Source --> **Recipient**)	**Recipient** Copy #	What Other Personal Data May the **Recipient** Have?
Pharmacy	• Demographic/Contact • Insurance • Prescriber ID (e.g., NPI) • Medication(s) prescribed and/or dispensed • MTM procedures (CPT)	Pharmacy requests payment for Millie's medication and for MTM services provided to Millie	Pharmacy --> **Millie PBM**	**I-15**	Other claims for Millie submitted to this PBM for adjudication

[8] Example of MTM claim form: https://www.bcbsal.org/providers/forms/pharmacyClaimForm.pdf.

o Millie's PBM may be allowed to de-identify the transaction and send de-identified data to the Pharmaceutical Manufacturer and/or sell it to a Pharmaceutical Market Intelligence Company. (The Pharmaceutical Manufacturer and Pharmaceutical Market Research Company each store copies of de-identified data, **copies DI-4;** "DI" designates "de-identified" data.)

Source of Data	Personal Data Transferred	Transfer Reason	Transaction Detail (Source --> **Recipient**)	**Recipient** Copy #	What Other Personal Data May the **Recipient** Have?
PBM	De-identified data	Generate revenue	PBM --> **Pharmaceutical Market Research Company**	**DI-4**	n/a

- Millie's PBM adjudicates the claim and sends it to Millie's Payer for payment. (Millie's Payer stores **copy I-16**.)

Source of Data	Personal Data Transferred	Transfer Reason	Transaction Detail (Source --> **Recipient**)	**Recipient** Copy #	What Other Personal Data May the **Recipient** Have?
Pharmacy	• Demographic/Contact • Adjudicated claim(s)	Payment of medication claim and MTM claim	Millie's PBM --> **Millie's Payer**	**I-16**	Other claims for Millie submitted to this Payer

- Millie's Payer sends Millie's adjudicated claims data ready for payment to a Third Party Administrator that pays the claims and sends Millie an Explanation of Benefits (EOB) detailing financial components of her visit with Dr. Smith including the amount billed, amount eligible for payment, insurance benefit paid or applied to deductible, and Millie's expected remaining balance due. (The TPA stores **copy I-17**.)

Source of Data	Personal Data Transferred	Transfer Reason	Transaction Detail (Source --> **Recipient**)	**Recipient** Copy #	What Other Personal Data May the **Recipient** Have?
Payer	• Demographic/Contact • Millie's adjudicated claims data	To enable the TPA to pay Millie's claim and send Millie an EOB	Payer --> **Third Party Administrator -> Millie**	**I-17**	Other adjudicated data about Millie

- Authorized as part of Millie's medical insurance plan, Millie's Payer sends a copy of Millie's prescription transaction along with other of Millie's PHI to a third-party Condition Management Company for program eligibility analysis and/or determination of appropriate care management protocol(s). (Disease Management Company stores **copy I-18**.)

Source of Data	Personal Data Transferred	Transfer Reason	Transaction Detail (Source --> **Recipient**)	**Recipient** Copy #	What Other Personal Data May the **Recipient** Have?
Payer	• Demographic/Contact • Insurance • Health claim type (e.g., Workman's Comp) • Prescriber ID (e.g., NPI) • Employment • Diagnoses • Procedures • Medication(s) prescribed	Determine Millie's eligibility for disease management program eligibility	Payer --> **Third-party Disease Management Company**	**I-18**	Data collected about Millie for past eligibility determination and/or additional personal data collected as part of another enrolled program

- Millie registers/signs-up for a PHR application provided by her employer.
  - o Millie authorizes her claims-based medication history data to be imported into her PHR. (Millie's PHR Company stores **copy I-19**.)

Source of Data	Personal Data Transferred	Transfer Reason	Transaction Detail (Source --> **Recipient**)	**Recipient** Copy #	What Other Personal Data May the **Recipient** Have?
PBM	• Demographic/Contact • Prescriber ID (e.g., NPI) • Medication(s) dispensed (claims data only)	Auto-populate Millie's plan-sponsored PHR	PBM --> **Third-party PHR Company**	**I-19**	Self-reported data entered by Millie

- Now Millie has her own electronic copy of the information, which she can forward to anyone of her choosing.

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.*

CP1 CP2 CP3 CP4 CP5 CP6 CP7 CP8 CP9

CT1 **CT2** CT3 CT4 CT5 CT6 CT7

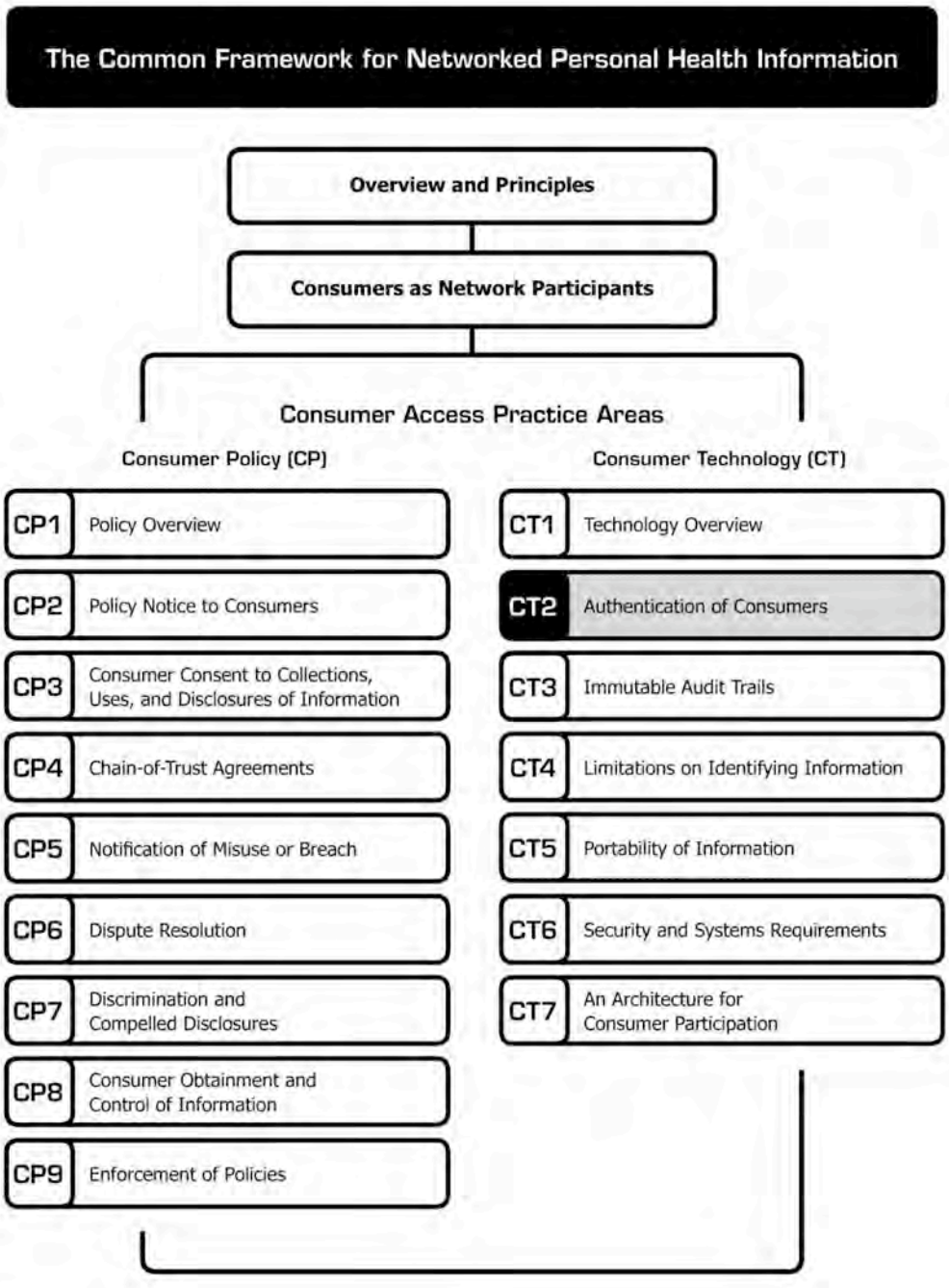
Authentication of Consumers

Authentication of Consumers

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:



Authentication of Consumers*

Introduction*

Trust in an electronic network depends on several factors, including assurances to consumers and participating entities that the information they access and share will be kept confidential, i.e., only shared with authorized actors. One key policy for achieving this trust, which is the focus of this paper, is to make sure that consumers are properly authenticated.

This work is the product of the **Connecting for Health** Work Group on Consumer Authentication Policies for Networked Personal Health Information.

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

6. Data Quality and integrity

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.

A Critical Problem of the Digital Age

At birth, a baby's hospital nametag is the first of several tokens that society will use to assert "identity" throughout the rest of life. For a child born into this Digital Age, countless electronic transactions will be based on assertions of identity. There is no practical or affordable technology — at least, not yet — to flawlessly identify each person for each transaction. So we use a variety of imperfect tokens (driver's licenses, passports, PINs, passwords, etc.) to validate an individual's claim to a particular identity. And that identity will be created over and over again in electronic systems throughout a person's life.

All business sectors and all individuals are challenged — and to some extent threatened — by this burden of proving identity, and of issuing and using authentication tokens. The increasing scattering of personally identifiable information makes identity management critical for business and consumer activities, yet at the same time problematic, costly, and sometimes risky. In the health care sector today, many important transactions occur daily with little rigor to confirm the identity of individual consumers.

This paper addresses the problem of authenticating consumers in electronic health information exchanges involving PHRs to ensure that each transaction is associated with the right person. These include concerns such as the growing public anxiety regarding privacy and security of personal health information, the fear by primary sources of data of increased risk to the information they hold, and loss of provenance of data, resulting from extensive sharing and duplication that could affect the trustworthiness of the system.

Because PHRs store sensitive personal health data, it is critical to develop reliable and trustworthy mechanisms to ascertain the identity of anyone accessing the information. Health information has several characteristics that make it even more sensitive than similar access to bank accounts and lines of credit, because someone who loses money through inappropriate access can be made financially whole. Someone who loses control of sensitive health data, by contrast, can never arrange to have that information returned to a purely private sphere. As part of handling this sensitive data, accurately identifying and authenticating

* **Connecting for Health** thanks Clay Shirky, New York University Graduate Interactive Telecommunications Program; Josh Lemieux, Markle Foundation; and Dan Combs, independent contractor, for drafting this paper.

consumers is an important hurdle to be overcome in enabling institutional health data sources to share electronic personal health information with consumer-accessible applications.

This paper offers a framework for processes by which participants in electronic health information networks can be assured that an individual consumer is who she claims to be. The framework includes these four components:

Identity Proofing: This is our umbrella term for the steps by which a person's identity is verified. Specifically, it is the validation of independent evidence and/or credentials of "identity." It happens several times throughout life at various institutions. For example, to receive a driver's license, a person must present required documents in person at a state motor vehicle department.

Identifiers or tokens: Once identity proofing is performed, organizations issue or require users to use tokens or identifiers, which could be physical documents (e.g., driver's license), biological markers (e.g., fingerprint), or be based on knowledge (e.g., passwords), or some combination (e.g., ATM card plus PIN).

Ongoing monitoring: After tokens have been issued or identifiers linked to an identity, systems are put in place to establish behavior patterns of individuals and alert authorized parties if behavior changes suspiciously.

Ongoing auditing and enforcement: If an organization relies upon third parties for identity proofing or the issuing of identifiers or tokens, then it must have mechanisms to audit those third parties and redress bad actions.

Note: The word "authentication" is sometimes used as an umbrella term for all of the above components to manage identity in an electronic environment.

Background

The **Connecting for Health** Work Group on Consumer Authentication Policies for Networked Personal Health Information focused on the authentication policies for private and secure consumer access to their health information routinely over the Internet to support important aims of consumer empowerment and improved health care quality and safety. Any framework for authentication in this environment must guard against opening up new vulnerabilities at a time in which medical identity theft already is a growing and serious problem.[1] Our Work Group's recommendations are consistent with principles articulated in the ***Connecting for Health*** *Architecture for Privacy in a Networked Health Information Environment*.[2]

See **Appendix A** for the membership of the **Connecting for Health** Work Group on Consumer Authentication Policies for Networked Personal Health Information.

See **Appendix B** for more detail on the scope and charge of this Work Group.

See **Appendix C** for the background and principles of **Connecting for Health**.

See **Appendix D** for a partial list of other groups working on the consumer authentication problem.

We use the following definitions in this paper:

- **Personal Health Records (PHRs):** PHRs encompass a wide variety of applications that enable people to collect, view, manage, or share their health information or health-related transactions electronically. Although there are many variants, PHRs are intended to facilitate an individual's ability to compile personal health information into an application that the individual (or a designee) controls. PHRs may contain copies of data held by health-related institutions as well as information contributed by the consumer or health monitoring devices. We do not envision PHRs as a substitute for the professional and legal obligation for recordkeeping by health care professionals and entities.
- **Consumer Access Services:** This is a set of functions that enable an individual consumer to securely access copies of their health data from multiple sources in an electronic

[1] *Medical Identity Theft The Information Crime That Can Kill You*, World Privacy Forum, Spring 2006. Accessed online May 2, 2007 at: http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf.

[2] Available online at: http://www.connectingforhealth.org/commonframework/docs/P1_CFH_Architecture.pdf.

environment. Consumers may be offered such services by a variety of organizations, ranging from existing health care entities to new entrants. Some will be covered under the Health Insurance Portability and Accountability Act (HIPAA), others will not. Consumer Access Services may combine both authentication services as well as data management services.

- **Health Data Sources:** For the purposes of this paper, a health data source is any entity that serves as custodian of the individual's personal health data. This may include health care providers and clinics, hospitals and health clearinghouses, pharmacies and pharmacy benefit managers, laboratory networks, disease management companies, and others that hold data related to the personal health of individuals.

The diagram below depicts a highly simplified data flow. In the center are Consumer Access Services, which include a mechanism to authenticate the individual consumer to the satisfaction of both ends of the exchange. (**Appendix F** contains a more detailed discussion of alternate models for conducting this authentication.)

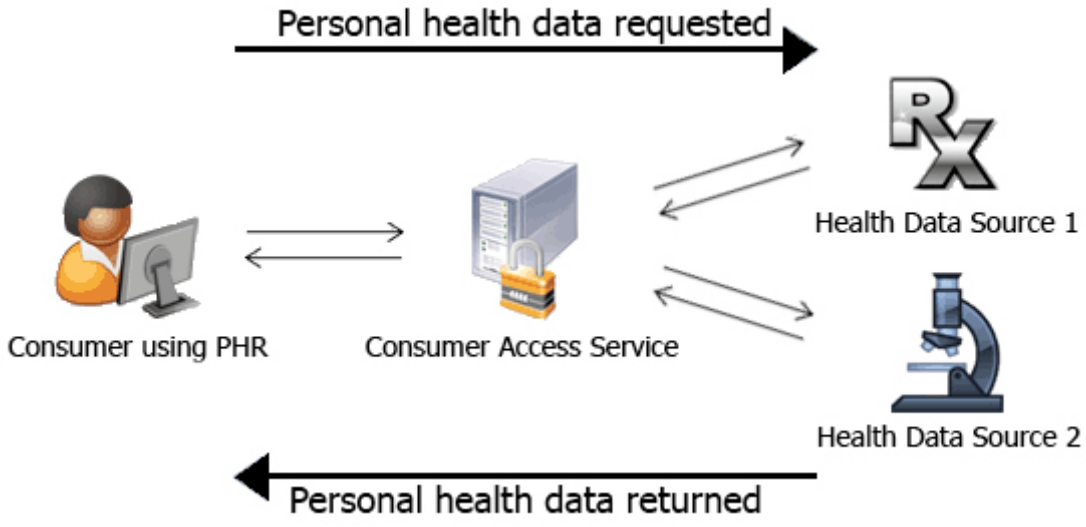
The simplicity of the diagram obscures a few important points about our vision for Consumer Access Services:

First, PHRs (i.e., consumer-facing applications) could be offered by entities at either end of the diagram. For example, an independent technology company (left side of diagram) could supply a PHR, and so could one or both of the health data sources (right side of diagram). The site of the application is not relevant. The aggregation of copies of data that the consumer collects could be stored at either end of the entities to exchange data, however, there needs to be what we call Consumer Access Services (including authentication and the provision of access to records).

Secondly and similarly, Consumer Access Services may be performed by a third-party intermediary, but they also could be performed by the PHR applications or the Health Data Sources, or both. In fact, the Consumer Access Services and the PHR may be offered by the same entity and therefore indistinguishable to the end user. Our concern is with getting the process of authentication right, without regard to what sort of entity is doing the authenticating.

Third, our recommendations are designed to be compatible with existing networks — health care providers forming electronic health information exchanges, pharmacy networks, or large non-geographic networks. As the *Networked Personal Health Information* paper points out, there is a great deal of electronically available personal health information in existing databases today. Existing networks (e.g., large scale pharmacy chains, the VA, Kaiser Permanente), Regional Health Information Organizations (RHIOs), or other new services (monitoring devices, disease management programs, etc.) emerging from continued innovation in the PHR space — all may eventually provide multiple avenues for consumers to receive copies of their health data.

Throughout its deliberations, our Work



Group was fully cognizant that other issues — revenue models, business relationships and contracts, limitations of liabilities, enforcement mechanisms — are bigger hurdles to PHR development than consumer authentication, which is the narrow focus of this paper.

Working Principles and Assumptions of the Work Group

In addition to the **Connecting for Health** principles (*see* ***Appendix C***), our Work Group agreed to the following guiding principles for solutions to the authentication problem:

Principle 1

Authentication systems should, as a whole, cover as much of the population currently using the U.S. health care sector as possible. Authentication processes that are ineffective or unavailable for particular groups of people (due to disability, expense to the user, lack of available credentials such as driver's licenses, etc.) should be balanced with alternatives appropriate for those groups, to the extent that such alternatives are available.

Principle 2

Consumers should have a choice in Consumer Access Services. Consumers should be entitled to a reasonable expectation of a choice of entities conforming to a published set of authentication standards. It's optimal, when feasible, to let informed consumers play a role in determining their Consumer Access Service provider and authentication stringency level of choice. However, given a widespread lack of consumer awareness about authentication techniques and identity threats, minimum consumer authentication standards for health information should provide relatively high security.

Principle 3

To be both effective and trustworthy, a distributed system of authentication needs oversight, accountability, and mechanisms of redress. The policies of the authentication system should be transparent. Systems should allow the consumer to understand who has potential access to her data as well as when it has been accessed and by whom, ideally on demand and in real-time.

We prefaced our deliberations by stating that:

- Our recommendations must be reasonably affordable and workable in today's environment.
- Our recommendations must not be tied to existing practices and technologies that may preclude future innovations.
- Our recommendations should not depend on the promise of future innovations in order for organizations to act on them now.
- Our recommendations must not favor any one technology or vendor, or any business model or business relationships.
- Our recommendations must be fully cognizant of any non-proprietary frameworks that are broadly accepted by at least large segments of the health sector.[3]

A Need for a New Approach

Frameworks that address the authentication problem typically do so based on a model of increasing stringency of identity proofing and authentication, corresponding with increased sensitivity of the data being accessed and the related risk. Requirements that are too low or loose create an unacceptable risk of the wrong person getting someone's information, compromising a consumer's accounts, defrauding providers or otherwise engaging in criminal acts. Requirements that are too stringent create unacceptable difficulties for the right person to get to his information, and may erect unacceptable barriers to adoption and implementation.

The development of networked PHRs is in its infancy, so there is no broad ecosystem to observe. Yet the problems of authentication are primarily ecosystem problems. If every organization dealing with a consumer managed

[3] On this final point, one key reference point for identity proofing and authentication stringency levels are those adopted by the E-Authentication Federation (EAF) among U.S. government agencies and its private sector companion organization, the E-Authentication Partnership (EAP). The National Institute for Standards and Technology (NIST) created a technical implementation guide for EAF based on industry standard Security Assertion Markup Language (SAML). The policies of the EAF have been licensed to the EAP.

its own authentication process from start to finish, there would be no systemic risk, and thus no need for a systemic solution. However, making every organization responsible for every one of its users pushes significant costs onto both the individual (who needs to manage multiple passwords) and the organizations that hold the consumer's data (each of which needs to be able to maintain a proofing and authentication infrastructure.)

A Consumer Access Service with insufficient proofing or authentication standards creates a risk for the security of the consumer's records. It also creates a risk to any clinical organizations and other entities that hold the consumer's data, to the degree that those organizations trust a Consumer Access Service to correctly validate a consumer's identity. If there is a race to the bottom for convenience to the customer, then there may be a high level of abuse (which could in turn inspire a draconian legislative or regulatory post-hoc remedy).

Therefore, it would be helpful to define an acceptable baseline identity proofing and authentication standard to which all Consumer Access Services should conform. Ideally, the standard would have an understood and generally accepted threshold for reliability, so that new methods for authentication can be evaluated against the effectiveness of existing methods. We aspire to a situation where an affordable and accepted industry standard is based on a measurable reliability of performance. However, as we discuss below, such a standard is not quantifiable today.

Given the constraints of the environment today, we make the following recommendations as an appropriate approach to the four key components of authentication: identity proofing, the issuing of identifiers or tokens, ongoing monitoring, and ongoing auditing and enforcement.

Component 1: Recommendations for Identity Proofing

The first step — verifying the identity of an individual consumer to an acceptable level of certainty — is typically the most difficult, expensive, and important.

Recommendation 1A: Consider in-person proofing as appropriate in some, but not all, cases: By in-person proofing, we generally mean requiring a face-to-face encounter in which the consumer presents a verified current primary government ID that contains a picture and either address of record or nationality (e.g., driver's license or passport). This option is an acceptable industry practice that is particularly appropriate when the organization performing the identity proofing:

a. Has no prior relationship with the consumer, and/or,
b. Has the infrastructure and budget necessary to conduct face-to-face encounters with consumers.

Discussion:

A key presumed advantage of requiring face-to-face identity proofing encounters is that it lowers the risk of mass or automatic attacks to obtain false credentials. In the virtual world, in which people can easily pose as others online, a requirement for in-person proofing has a strong appeal: It seems like the best way to establish a baseline identity of an individual. It raises the presumed commitment of the individual submitting to the proofing process. It raises the cost of a conducting a fraudulent "attack" on an individual identity, and it reduces the likelihood of remote, automated attacks from many sources or on many identities at once. Requiring presentation of commonly used documents (e.g., birth certificates, driver's licenses, and passports) sets a hurdle for registrants and brings into play a variety of laws that may be useful at a later time for enforcement or prosecution, if necessary.

Caveats:

However, this option comes with three critical caveats:

- First, although dissuading misuse is a key goal for any such system, these same hurdles dissuade legitimate use as well. In-person proofing carries a cost and inconvenience burden for consumers, particularly those who face mobility or transportation barriers. Given the potential utility of providing consumers with electronic access to their health

information and services, this outcome is not ideal and risks systematic underuse of PHRs. In-person proofing may be in tension with Principle 1, above, that the authentication process be available to as much of the population as possible.

- Secondly, in-person identity proofing is a significantly costly and labor-intensive process, which many organizations are not well-positioned to perform. If in-person identity proofing were required of all organizations on the network, it would keep organizations that could offer potentially useful data or services from participating. This affects both large and small organizations. For example, the Centers for Medicare & Medicaid Services (CMS) — the nation's largest payer — has no direct way currently to conduct face-to-face identity proofing of its beneficiaries. Nor do most technology companies or web portals ever conduct in-person encounters with their customers.
- The third — and most critical — caveat is that, although in-person processes are a widely accepted starting point for identity proofing, we could not find (much less validate) any measurement of their effectiveness. If there were such a measurement (in the manner of "errors per 100,000" or similar), it would enable useful comparisons between various forms of in-person proofing, and between in-person and remote forms of proofing. Our Work Group found a dearth of publicly available research backing up the accuracy of in-person proofing. The assumption that in-person proofing is acceptably accurate is not based on empirical understanding. And certainly, the stringency of methods for in-person proofing varies from one organization to another. In fact, the existence of an in-person proofing process may create a false sense of security if those checking credentials are not well-trained or audited. Recommendations 1B, 1C and 1D below attempt to address this problem.

Approach 1B: Consider 'bootstrapping' of in-person proofing by other organizations: We recommend that entities in the health sector consider "bootstrapping" other in-person encounters by third-parties to establish the consumer's identity at acceptable levels of accuracy. We recommend that both current and potential holders of clinical data consider partnering with institutions that have effective authentication processes.

Discussion:

For many reasons, individual doctors' offices are not well-equipped to authenticate 300 million Americans. (Their main authentication procedures relate to confirming eligibility for health benefits.) However, there are other common places where in-person proofing can occur, including post offices, retail pharmacies, notary publics, and financial institutions. In the bootstrapping model, a laboratory could accept the authenticated identity of a consumer who had first been authenticated by another one of these parties. The entity would pass at least the assertion that the patient has authorized a copy of the medical records to be transferred. Note that if a system passes demographic details, it should never re-use existing identifiers. It would be potentially catastrophic, for example, to bind a consumer's PHR directly to a bank account number, as publication of the number would then compromise both categories of data.

This is not a general-purpose solution, as the issues of transparency and liability will have to be worked out as business relationships between the authenticator and the relying party that holds the consumer's health data. However, it would allow new interfaces to be offered to consumers for access to their records, and would do so without creating new proofing hurdles. (These kinds of relationships will probably form as point-to-point business agreements, rather than multilateral networks, at least at first.)

Approach 1C: Consider alternatives to in-person proofing: Because there are no metrics to evaluate the quality of existing proofing systems, the data holder is, de facto, left to judge the acceptability of various methods. We recommend that data sources consider adopting remote proofing on their own, or rely on remote proofing from acceptable third parties (*see Component 4 section below*), when such proofing methods:

a. Rely on combinations of at least two alternative methods or sources for validating identity that use separate data (i.e., don't use two different sources relying on Social Security Number or the same account number).
b. Are optimized to minimize the rate of false positives (i.e., when the wrong person is granted access based on an identity not his own).
c. Provide an alternative identity-proofing protocol to mitigate false negatives (i.e., when the right person using his correct identity is denied access nonetheless). In such cases, the person denied access in a remote-proofing protocol should be given an alternative means, such as in-person, to establish that he really is who he says he is.
d. Take precautions to minimize risk to the consumer, including but not limited to:

    - Not requiring consumers to use existing account numbers as identifiers. After the initial proofing step, nothing should be communicated from the consumer to the identity proofer that could provide access to the consumer's account if intercepted by a third party.
    - Securely storing and limiting the number of parties privy to any "shared secrets" (*see page 8*) to the absolute minimum necessary.
    - Refreshing interrogation questions and "shared secrets" so as to avoid overuse.

This is not meant to be a list but a guide. Security practices change, and the underlying concern should be to adopt practices that create the necessary security while minimizing the privacy risks of the security methods themselves.

Discussion:

Knowing when remote proofing is acceptable suffers from a Catch-22. The obvious threshold for remote proofing should be, at a minimum, "as good as or better than current practice." However, since there are no convincing metrics for current practice, it is impossible to say how any remote proofing system compares. With fake IDs readily available and with harried clerks often doing the checking, in-person identity proofing does not guarantee that any particular individual is who he claims to be. In some cases it is possible that remote proofing actually works better in defending against a determined attacker than current in-person proofing practices.

There are examples, as with PayPal, where user-proofing is transactional (i.e., based on past or present transactions of information or money that serve to tie a person's identity to a location or service, such as a U.S. Mail box or a bank account), and requires no face-to-face encounter. This method is one of a subset of "Knowledge-based Authentication" (KBA) methods in which a consumer is identified by answering a set of questions only she could reasonably be assumed to know. Sometimes these questions involve historical information (past addresses, use of credit cards for certain transactions) and sometimes they involve information generated as part of the KBA process itself, as with the PayPal technique of generating specific deposits.

The ideal situation would be to measure effectiveness of proofing by a numerical target, such as: "Wrongful issuance of credentials must be kept to an error rate below one in X," where X would be at least a thousand patients. (This metric would be a 99.9% deflection of false positives, in other words.) In the absence of such precision, for either in-person or remote proofing (*see 1D, below*), the decision about when and how to use remote proofing will necessarily be in the hands of the person responsible for the security of patient data, to be undertaken with two principles in mind: Minimize false positives, and don't rely on a single method.

Our recommendation is that at least two methods or sources be used in remote proofing processes. (For example, the consumer presents authentication credentials issued to him by another institution and successfully responds to an online interrogation about information acquired through his relationship with a separate independent service.) This is because two methods are likely to have different strengths and weaknesses, thus raising the cost of an attack while lowering its chance of success. This is true for both defense (i.e., it's less likely that a criminal could fraudulently obtain knowledge or credentials in two places

than in one) and for sustainability (i.e., if one method becomes compromised, the system would still have at least one untainted method still running, to which it could add new methods without starting from scratch).

Approach 1D: Begin Federal research on identity proofing quality: This is not a recommendation to data holders, but to the federal government. We recommend that the National Institute of Standards and Technology (NIST), in collaboration with other interested agencies, study current identity proofing practice wherever consumers are given access to their records remotely to provide or create metrics expressing the effectiveness of those various methods.

Discussion:
The current administration has made increasing accessibility of electronic health records to providers and citizens a national goal, and the lack of well-understood and generally agreed-to authentication methods for consumers is clearly a hurdle. This recommendation is intended to lead to a benchmark for future proposed systems to meet or exceed, thus moving us out of the current situation of identity proofing ratified by habit, but uninformed by measurement.

Recommendation 1E: Do not use clinical data in the proofing process: As a matter of privacy policy, we recommend against using clinical data as validation data in a proofing process. The reasons for this are articulated in the **Connecting for Health** paper *Linking Health Care Information: Proposed Methods for Improving Care and Protecting Privacy*.[4]

[4] Available online at: http://www.connectingforhealth.org/assets/reports/linking_report_2_2005.pdf.

Component 2: Recommendations for Issuing Tokens or Identifiers

Upon successful completion of identity proofing, it is necessary to issue acceptable tokens or identifiers to the consumer.

Recommendation 2A: Bind the consumer's identity in such a way as to facilitate later authentication: At the time of initial proofing, the capture and retention of copies of the documents allows for re-verification if needed at a future time. If in-person visits are used in identity proofing, they present an opportunity to capture a biometric indicator, such as photographs or fingerprints.

Discussion:
This process of connecting or binding of particular information or attributes to a particular physical person, when combined with system monitoring, can provide improved ability to discover certain types of fraud attempts in which attributes are used by multiple registrants. However, it is important to note that improved information collection, of any sort, also raises the requirements for securing the database where the records are stored. Improvements in knowledge-based authentication methods generate, as an inevitable side effect, more stored knowledge about the consumer — knowledge that must be held securely to prevent near-term defeat of the authentication system itself and to prevent identity theft. Although database security is not in the scope of this paper, we note that care must be taken to evaluate the security of the data held in aggregate, as well as the security of person-by-person authentication.

Less reliable, although at times more economically practical, are password reminders as "shared secrets" that can be used to support later authentication, or password reset requests. A common example is for the consumer to be forced to answer questions such as pet names or mother's maiden name. Care must be taken that these not be based on common questions that can be easily guessed or snooped. Another possible source of shared secrets are questions the service asks of the consumer. For example, PayPal makes two small deposits in a new user's

account, then asks that the user report those amounts back to PayPal. This removes the risk of trivial guessability, though it requires a higher degree of integration with the financial system.

Interesting work is being done on "zero-knowledge" authentication systems, which reduce or eliminate the need for knowledge-based secrets to be held by the authenticating party. In a zero-knowledge system, the consumer proves who he is by using a secret that only he knows to perform a task that he could only perform with that secret. (Imagine that you see someone unlock a door that you know can open with only one key. You could conclude that the person has that particular key without you needing to see a copy of the key yourself.) "Zero-knowledge"-based systems have not yet been widely deployed, and have significant management issues in their current implementations. Still, they should be watched closely, as they may provide a way to increase authentication security without also increasing the privacy risk to consumers that comes with knowledge being held about them in various authentication databases.

Recommendation 2B: Choose an appropriate token or identifier: There are a variety of credentials available. PINs, cards, tokens, fobs with RF chips, antennas, and fingerprints are a few examples of a rapidly growing array of tokens.

Discussion:

Many different types of tokens or identifiers can be used to good effect in authentication processes. Much depends on the budget and infrastructure of the token-issuer and the tolerance of consumers to remember and use the token appropriately.

Recommendation 2C: If using passwords as tokens, enforce 'strong' passwords: Requiring and enforcing rules to create strong passwords[5] — i.e., passwords that are not easily guessable — is one of the first relatively easy steps that will dramatically increase the security of the username and password token.

Discussion:

The username and password combination is the most commonly used token. Extremely valuable and potentially risky transactions are conducted millions of times each day employing the protection of username and password. Many of the tokens and identifiers listed in Recommendation 2B are essentially variations on the concept of username and password, incorporating a variety of technologies to improve on the basic concept. Used appropriately, the username and password combination provides significant protection at very moderate cost and user inconvenience. However, if unguided by a set of guidelines or password requirements, many consumers tend to create easily guessable passwords and otherwise create the opportunities for compromise of their identity.

Many systems now prevent the use of dictionary terms as passwords, or consecutive or repeating strings of numbers or letters or other easily guessable phrases. Some require the use of at least one number, a letter and another

[5] The following documents contain useful information about the issuing of tokens, including strong passwords:

NIST Special Publication 800-63: Appendix A-Estimating Password Strength and Entropy, pp. 46-53. Table A-1: Estimated Password Guessing Entropy in bits vs. Password Length, p. 53. Accessed online on May 3, 2007, at: http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf.

Password Strength, Wikipedia. Available at: http://en.wikipedia.org/w/index.php?title=Password_strength&oldid=154706929.

National Institutes for Health, Password Policy for eRA. Accessed online on May 3, 2007, at: http://era.nih.gov/docs/NIH_eRA_Password_Policy.pdf.

NIST Special Publication 800-12: Chapter Sixteen – An Introduction to Computer Security – The NIST Handbook: Identification and Authentication. Accessed online on May 3, 2007, at: http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter16-printable.html.

keyboard character. Some systems will provide a rating of the strength of the password as it is created by the user. The fundamental challenge with strong password requirements is that they not only make it harder for illegitimate users to guess a password, they can make it harder for the legitimate user to remember it. If strong password requirements are too onerous, they may encourage legitimate users to compensate through insecure practices, such as writing down a password and leaving it next to an unattended computer.

It is increasingly common to supplement the username and password combination with monitoring of the requesting machine (e.g., source IP address, machine and browser characteristics). Such monitoring, which we discuss further below, requires no additional issuing of tokens to the user.

Recommendation 2D: Limit attempts on passwords: Given sufficient time, access, and attempts, any password will eventually succumb to attempts to guess it. Limiting the number of consecutive and total attempts to enter a password, requiring periodic changes to the password, and other relatively low-cost, relatively low-inconvenience requirements for use of passwords make password guessing an unacceptably difficult approach to compromising tokens.

Recommendation 2E: Establish a clear policy on requirements for password changes: Although an inconvenience to end users, it may be reasonable to require consumers to create new passwords at regular intervals. Each system should decide locally whether to enforce a policy requiring that consumers change their passwords over time. However, if such policies are enforced, it's critical that consumers be given clear explanations on the methods and reasons for resetting their passwords.

Discussion:

The value of tokens can diminish over time. For example, many private and government organizations still use Social Security numbers not only as identifiers but also as tokens,[6] and it is precisely because of this ubiquity of uses that Social Security numbers have been a boon to identity thieves. Similarly, if a consumer uses the same password and password reminder at every site visited, it is much less secure than if the consumer uses different secret codes at each site's login. On the other hand, consumers may have trouble coming up with strong passwords that they can remember, and the burden of having to do so frequently could drive down utilization. The value of forcing consumers to change passwords is hotly debated, and our work group did not feel strongly about making a recommendation one way or the other.

Component 3: Recommendations for Ongoing Monitoring

It is important to perform periodic or ongoing processes to continually improve upon the initial proofing and to weed out compromised identities.

Recommendation 3A: Conduct appropriate ongoing monitoring: Ongoing monitoring is an essential third component of appropriate authentication because of inherent weaknesses in the first two components (i.e., identity proofing and issuing of tokens). Given the widespread compromise of documents used for initial identity proofing and the large and growing incidence of identity crimes, the function of authentication should be thought of as an ongoing process rather than a gateway to be passed through one time. Once the consumer's identity is proofed and the token is issued, systems should establish the behavior patterns of individuals and alert authorized parties when behavior falls out of the established pattern. For example, credit card

[6] The principal reason Social Security Numbers (SSNs) should not be used as tokens is that, if this approach is taken, then one number is used to provide the public and secret parts of authentication (i.e., you have an SSN that points uniquely to you, but you must reveal it as proof that you have it.) Without being accompanied by a second, secret token such as a PIN, the SSN is damaged in regard to authentication by the very use that makes it otherwise worthwhile. In addition, no one token should be relied on too heavily, as such ubiquitous use will increase the focus of malevolent actors on compromising that token, and any compromising of such a token will have disproportionately negative effects.

companies have algorithms to detect sudden changes in charging behavior, triggering a telephone call to the consumer to investigate possible fraud.

Discussion:

Identity proofing is often used as a "gateway" process. It is merely a perimeter defense, performed once and not revisited. Once identity proofing is completed, a registrant is an "insider" of the system. And there is often much secondary reliance on this initial proofing, such as airport security relying on a state-issued driver's license. In the Digital Age, the outside/inside relationships change continually. Allowing network access to partners, customers, users, and some unintended participants quickly renders perimeter defenses insufficient. Additionally, much of the fraud and abuse comes from people accurately identified or from identities that were compromised after the initial proofing process, as well as from "inside" authorized users.

There is a robust and active population that continually probes and prods for opportunities to compromise systems and almost immediately shares with others any new intelligence gained. The risks and threats to systems change continuously. The practices and processes to respond to these threats must likewise change.

The automated ability to monitor individual behavior for fraud varies significantly from organization to organization, depending in part on the type of organization, what data it captures, and what it is permitted to do with the data. Valuable techniques include analysis of transaction history and location, keystroke patterns, and others. Detailed recommendations would rapidly become dated and ineffective. Decisions about an ongoing monitoring process must be made locally. The U.S. government provides some guidance for ongoing monitoring as an integral part of an authentication process in the *NIST Special Publication 800-100, Information Security Handbook: A Guide for Managers.*[7]

Behavior pattern monitoring can include information about the method of login (e.g., consumer's usual IP address, machine and browser type, etc.), or information about the types of resources or data that the consumer typically accesses.

Recommendation 3B: Enable consumers to view an immutable audit trail: Consumers can become powerful allies in detecting identity fraud when they have access to the transaction history of their accounts. We recommend that Consumer Access Services and PHR offerers provide authenticated consumers with online access to an immutable audit log displaying all accesses and data transactions involving their account.

Discussion:

Consumers now are able to review their own credit reports online, providing an important and highly invested check on potential fraud or errors. This recommendation is in keeping with Principle No. 3 of this document. The **Connecting for Health** Common Framework document, *Auditing Access to and Use of Health Information Exchange*, provides some guidance in this area of immutable audit.[8]

Component 4: Recommendations for External Audit and Enforcement

When relying on a third party to perform proofing or issuing of tokens, or both, some mechanism of audit and redress is essential to establishing a chain of trust.

Recommendation 4A: Ensure that third parties are "observable" in how and how well they are performing identity proofing, token-issuing, and ongoing monitoring or any related services to authenticate consumers. One recommended practice is to have a contractual commitment for the parties to notify each other if either detects system compromise above a certain threshold or fails to comply with agreed procedures.

[7] *NIST Special Publication 800-100 - Information Security Handbook: A Guide for Managers*, pp. 14-15. Accessed online on May 3, 2007, at: http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf.

[8] Available online at: http://www.connectingforhealth.org/commonframework/docs/P7_Auditing_Access.pdf.

Discussion:
A fundamental premise of the *Common Framework for Networked Personal Health Information* paper is that Consumer Access Services will emerge to help consumers "network" their PHRs with connections to multiple sources of health data and services. In order to facilitate the consumer's requests for digital copies of his information from Health Data Sources, all parties must be assured of the individual's identity and bona fide authorization to share data. Simply put, such transactions require "trust."

It will be impossible to trust and rely on any third-party's authentication if those third-parties' practices are not observable either directly among contracted parties or via some industry-accepted auditing and validation mechanism.

Recommendation 4B: Ensure a mechanism for enforcement and redress for bad actions: There needs to be a commonly accepted mechanism, agreed upon in advance, to redress unacceptable practices and eject bad actors.

Discussion:
Audit, enforcement, and redress are general issues for Consumer Access Services, not just with the task of authentication. All this is framed against the larger issues of binding Consumer Access Services to policies and accountability generally, and against the general fragmentation of the health care industry (a fragmentation that may increase as Consumer Access Services enter the picture).

Recommendation 4C: Consider federation and/or other contractual means to address Recommendations 4A and 4B:

If the Health Data Source:

- Has not done its own identity proofing and token-issuing for a consumer, and;
- Is considering a request from a Consumer Access Service to pass information on the consumer's behalf, and;
- Does not have sufficient direct means to monitor or observe the Consumer Access Service's authentication practices per Recommendations 4A and 4B...

Then, we recommend that:

- The Health Data Source should have strong mechanisms in place for identifying the Consumer Access Service itself.
- The Consumer Access Service should be contractually bound to policies or to a group that sets and enforces shared policies, (e.g., the E-Authentication Federation (EAF), Electronic Authentication Partnership (EAP), or similar.)
- The Consumer Access Service should use at least EAP Level 2, or equivalent.

We believe the EAF/EAP is a good framework for a discussion on finding an acceptable degree of authentication certainty and policy enforcement. Although some organizations might choose to join the EAF or the EAP, there is likely no one-size-fits-all answer. Different business relationships and different consumer populations will likely require a variety of authentication services for their transactions. Some consumers may even demand higher-level authentication stringency for certain services.

Discussion:
We emphasize that the above scenario is not the only way to approach the problem. (*See **Appendix F** for a draft architecture discussion.*) Point-to-point trust is conceptually simplest from the point of view of any given pair of actors, but pairwise trust exposes the system as a whole to daunting complexity. Similarly, a single national actor coordinating trust on behalf of everyone is not feasible at this time, both because of the realities of fragmentation and the business context, and also because the policing problem for a single actor is acute. If these two extremes are in fact impractical, this suggests some sort of chain of trust with mutual policing, with various actors monitoring one another, possibly in contractually arranged groups.

Conclusion: A Path Forward

This paper is driven by a desire to allow U.S. consumers to access and gain value from their own health information. **Connecting for**

Health accepts that much of our valuable personal health data is stored and managed by numerous entities. The next key challenge is to establish the rules and techniques that establish trust among participants over a "network of networks."

Policy rules will be needed in a number of areas — including patient consent, secondary use, and data management. Identity has quickly emerged as a primary problem in network access — particularly given the sensitivity of personal health information. A well-understood and implemented Common Framework for managing health consumers' identity is a prerequisite to networked use of personal health records.

The recommendations in this paper are based on the technologies and practices current at a particular moment, and our desire to stimulate national progress in addressing this particular obstacle to consumers' electronic access to their health information.

The problems of identity proofing and authentication are widely felt by all industries handling sensitive data or electronic transactions, and as a result, there is rapid evolution in the tools available for authentication. Any process of authentication for consumer access anywhere in health care must be regularly re-evaluated to factor in both new threats and new capabilities.

Many health care entities have significant interest in some form of networked personal health records. The relationships they forge could have significant impact on possible trust scenarios for consumer authentication. In addition, there is a critical need to expand consumer education about techniques to safeguard identity in the Information Age. Consumers should understand, first, that there are tradeoffs between security and convenience and, second, what the tradeoffs mean for them.

These many trends — new threats, new business relationships, emerging technologies, and consumer awareness and behavior — all warrant close monitoring. They certainly will have more impact on future health information sharing environments than the modest recommendations in this paper. We do, however, hope that this paper contributes to a growing consensus that the path forward on consumer authentication requires careful thinking, new research, and innovative approaches.

Appendix A: Acknowledgements

Connecting for Health thanks the following Work Group members for participating in the rich discussion that resulted in this paper.

Chair

Clay Shirky, New York University Graduate Interactive Telecommunications Program

Work Group

Paula Arcioni*, New Jersey Office of Information Technology

Ernie Argetsinger, Omnimedix Institute

Siddharth Bajaj, VeriSign, Inc.

Dan Combs, Global Identity Solutions, LLC

Jeremy Coote, InterComponentWare, Inc.

Maureen Costello, Ingenix

Phillip D' Angio, VeriSign, Inc.

James Dempsey, JD, Center for Democracy and Technology

Carol Diamond, MD, MPH, Markle Foundation

Martin Fisher, MedicAlert Foundation International

Thomas Foth, Pitney Bowes, Inc.

Christopher Gervais, Partners Community HealthCare, Inc.

Mark Gingrich, MS, RxHub, LLC

Janlori Goldman, JD, Health Privacy Project

Philip Hagen, MD, Mayo Clinic

Jonathan Hare, Resilient

Elizabeth Holland*, Centers for Medicare & Medicaid Services

Mark Johnson, Vanderbilt University and Medical Center

Jennifer Kerber, Information Technology Association of America

Kristy LaLonde*, Office of E-Government, Information Policy, and Technology
U.S. Office of Management and Budget

David Lansky, PhD, Markle Foundation

J.P. Little, RxHub, LLC

Kathleen Mahan, MBA, SureScripts

Georgia Marsh*, United States General Services Administration, E-Authentication Initiative (former position)

Phil Marshall, MD, MPH, WebMD Health

Daniel Matthews, Lockheed Martin Corporation

Damon Miller, CapMed Corporation, A Division of Bio-Imaging Technologies, Inc.

Kim Nazi, FACHE*, United States Department of Veterans Affairs

Alison Rein**, AcademyHealth

Eric Sachs, Google Health

Charles Safran, MD, Harvard Medical School

Scott Schumacher, PhD, Initiate Systems, Inc.

Donald Simborg, MD, Independent Consultant

Michael Simko, RPH, Walgreens Pharmacy Services

Michael Stokes, Microsoft Corporation

David Temoshok*, General Services Administration, Office of Governmentwide Policy

Robert Tennant, MA, Medical Group Management Association

Jeanette Thornton, MPA, America's Health Insurance Plans

Allison Viola, American Health Information Management Association

David Yakimischak, SureScripts

The **Connecting for Health** Work Group on Consumer Authentication Policies for Networked Personal Health Information wishes to thank **Josh Lemieux** for his expertise and tireless help preparing this manuscript. In addition, we thank **Clay Shirky** for his leadership and work on this manuscript. Without his unique ability to parse very complex issues carefully and adeptly, we could not have achieved this paper. We also thank **Dan Combs** and **Stefaan Verhulst** for their help researching and drafting portions of this document.

*Federal and state employees participated in the Work Group but make no endorsement.

**Participated in Work Group but makes no endorsement per employer policy.

Appendix B: Scope and Charge of the Work Group

The Work Group on Consumer Authentication and Health Information Exchange was charged with defining a framework to authenticate the identity of individual consumers consistent with **Connecting for Health** principles. This includes identifying a baseline of policies and technologies to assert, within acceptable thresholds of accuracy, the identity of an individual consumer requesting copies of her personal data in an electronically networked health information environment. The recommendations are intended to encourage a fresh approach to foster trust of all network participants, and specifically to protect the consumer, the health data holders, and the Consumer Access Services from the following threats:

- **Defense against illegitimate access to health records:** This is defined in this paper as externally targeted or automated attacks to gain access into an individual's health information. The attackers in this scenario could be either known to the consumer (as with a relative or colleague looking at material inappropriately), a targeted attack by someone not known to the patient (as with a private detective trying to access records), or an indiscriminate attack (someone looking for anyone's health records, possibly as a precursor to medical fraud).
- **Defense against identity theft:** The threat here is not to the clinical data per se, but to the consumer's identifiers and demographics — address, date of birth, Social Security Number, health benefit eligibility number, etc. Protecting against identity theft is an obvious goal. The key complication here is that it is very difficult to protect against family members posing as one another, and it is not possible to design a system that covers all state regulations of parental access to their children's data. Our Work Group did not focus on proxy access beyond the key principle that the identity of all proxies accessing the system be recorded, as well as the identities of people for whom they are proxies, so that, should a proxy later lose access, their authentication tokens can be revoked separately from the main account.

The following issues fell outside of the scope of this Work Group, but we list them here to acknowledge their importance in creating a trusted health information sharing environment for consumers:

Consumer Issues:

- **Consumer Behavior:** We are not addressing what consumers do with their copies of personal health data. We live in an age in which individuals are increasingly self-publishing on the Internet intimate details of their personal lives. It was outside the scope of this Work Group to attempt to address the complexities of individual behavior and choice. Nevertheless, these are relevant concepts. Consumers' own experiences and individual preferences will no doubt shape this emerging area.
- **Phishing:** There is a parallel problem to consumer authentication, related to the assurances provided by the entity hosting the consumer's data. Mechanisms need to be in place to defend the consumer against "phishing" attacks, where a consumer is directed to log into a seemingly legitimate web site or service, but which is really a copy of an existing site, with a similar URL. The risk of such phishing in medical contexts is high; however, the defenses against the phishing problem require a different set of strategies than those outlined in this document.

Data Storage Issues:

- **Data Security:** Methods to encrypt and secure health data repositories are beyond the scope of this paper. We focus on defense against unauthorized users defeating authentication systems, not attacks on larger data stores. For purposes of this paper, we accept as a precondition that all actors have good physical security practices. The digital signing of records is also outside the scope of this paper.
- **Data Policies:** Also out of scope of this paper are policies for data custodianship and data sharing other than those related to identity

proofing and authentication. The parallel Connecting for Health Work Group on Consumer Access Policies for Networked Personal Health Information is working on recommendations for privacy policy, disclosure and consent, secondary use, etc. For purposes of this paper, we accept as a precondition that the consumer has voluntarily initiated a PHR account and authorized all uses and exchanges of personal health data consistent with **Connecting for Health** principles for privacy.[9]

Business Issues:

- **Business relationships:** This paper does not address the necessary business relationships that would provide motivations for health data sources and PHR services to share data on the consumer's behalf, or for intermediaries to emerge between them.

In summary, this paper focuses on a framework for the authentication process when the individual wants to access or contribute personal health information electronically among health professionals or other health-related entities (HIPAA-covered or not).

[9] Available online at: http://www.connectingforhealth.org/commonframework/docs/P1_CFH_Architecture.pdf.

Appendix C: Background on Connecting for Health

Connecting for Health, founded and operated by the Markle Foundation, with additional support over the years from the Robert Wood Johnson Foundation, is a public-private collaborative organization with representatives from more than 100 organizations across the spectrum of health care stakeholders. Its purpose is to catalyze the widespread changes necessary to realize the full benefits of health information technology (HIT), while protecting patient privacy and the security of personal health information. **Connecting for Health** is continuing to tackle the key challenges to creating a networked health information environment that enables secure and private information sharing when and where it's needed to improve health and health care.

Connecting for Health has produced the following documents that lay the groundwork for this current work product focused on consumer authentication:

- ***Linking Health Care Information: Proposed Methods for Improving Care and Protecting Privacy (February 2005)*** — which describes an approach to matching patient records among disparate health care institutions.[10]
- ***Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange*** (April 2006) — which elaborates and defines a set of policy and technical elements necessary to enable secure exchange of health records among providers across the Internet, including a set of principles for privacy and fair information practices in a networked environment. The **Connecting for Health** Common Framework is composed of nine policy documents on topics such as privacy, notification, audit, and authentication of non-consumer users of the network, and six technical documents that elaborate technical specifications of a network approach based on those policies.[11]

[10] Available online at: http://www.connectingforhealth.org/assets/reports/linking_report_2_2005.pdf.

[11] Available online at: http://www.connectingforhealth.org/commonframework/index.html.

- ***The Architecture for Privacy in a Networked Health Information Environment*** (April 2006) — which describes a set of fair information practices that the Common Framework has endorsed to guide systems that support the exchange of personal health information. These principles are:
  - **Openness and transparency:** Consumers should be able to know what information exists about them, the purpose of its use, who can access and use it, and where it resides. They should also be informed about policies and laws designed to ensure transparency on how privacy is assured.
  - **Purpose specification and minimization:** The purposes for which personal data are collected should be specified at the time of collection, and the subsequent use should be limited to those purposes or others that are specified on each occasion of change of purpose.
  - **Collection limitation:** Personal health information should only be collected for specified purposes and should be obtained by lawful and fair means. Where possible, consumers should have the knowledge of or provide consent for collection of their personal health information.
  - **Use limitation:** Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified.
  - **Individual participation and control:** Consumers should be able to control access to their personal information. They should know who is storing what information on them, and how that information is being used. They should also be able to review the way their information is being used or stored.
  - **Data quality and integrity:** All personal data collected should be relevant to the purposes for which they are to be used and should be accurate, complete, and current.
  - **Security safeguards and controls:** Personal data should be protected by reasonable safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure.

- **Accountability and oversight:** Entities in control of personal health information must be held accountable for implementing these principles.
- **Remedies:** Legal and financial remedies must exist to address any security breaches or privacy violations.

Connecting Americans to Their Health Care: A Common Framework for Networked Personal Health Information (December 2006) — which envisions a consumer-accessible data stream, consisting of electronic copies of personal health data that have been captured at various points on a network (e.g., doctor's offices, hospital systems, pharmacies and pharmacy benefit managers, labs, diagnostic imaging services, etc.).[12]

[12] Available online at: http://www.connectingforhealth.org/commonframework/docs/P9_NetworkedPHRs.pdf.

Appendix D: Other Groups Working on Authentication

The following paragraphs list several authentication projects that currently exist. This list is based on input from Authentication Work Group members and is not comprehensive.

Electronic Authentication Partnership (EAP)

Building off the work of the E-Authentication Federation (see below) and other authentication federations, EAP has developed as a "multi-industry partnership working on the vital task of enabling interoperability for electronic authentication among public and private sector organizations." It is sort of a federation of federations. This group is creating a framework for accrediting and compliance testing of participating Credential Service Providers (CSPs) and Relying Parties (RPs). EAP also addresses the issue of liability.

See: http://eapartnership.org/

See Trust Framework web site: http://www.eapartnership.org/docs/Trust_Framework_010605_final.pdf

E-Authentication Federation

The E-Authentication E-Government Initiative is one of the President's 24 cross-agency E-Government Initiatives. Its mission is to put in place the necessary infrastructure to support common, unified processes and systems for government-wide use. E-Authentication recently launched the E-Authentication Federation (EAF), "a public-private partnership that enables citizens, businesses, and government employees to access online government services using log-in IDs issued by trusted third parties, both within and outside the government." Currently 13 different agency web applications are using the service. EAF has focused on the creation of policies, systems, and relationships that reuse existing credentials to meet the needs of mostly federal government-relying parties. EAF has created a framework by which a variety of Credential Service Providers — currently including federal, state, and private sector organizations — issue credentials to be trusted by Relying Parties in the federal government.

(Quotations taken from E-Authentication web site: *http://www.cio.gov/eauthentication/)*

Privacy:
http://www.cio.gov/eauthentication/documents/EAprivacy.htm

E-Authentication Guidance for Federal Agencies (M-04-04):
http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

NIST 800-63: E-Authentication Technical Guidelines:
http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

NIST 800-53: Recommended Security Controls for Federal Information Systems:
http://csrc.nist.gov/publications/drafts/draft-SP800-53.pdf

Liberty Alliance Project

In 2001, a consortium of 30 organizations formed the Liberty Alliance Project. The project's stated mission is: "to establish an open standard for federated network identity through open technical specifications." Over the past few years, they have published an "open framework for deploying and managing a variety of identity-enabled Web Services." Liberty Alliance is currently working on a framework for "deploying and managing interoperable strong authentication."

Liberty Alliance is a standards group. Liberty Alliance is represented on the EAP and involved either directly, or through efforts of members and the products and services they provide, with the other efforts.

(Quotations taken from Liberty Alliance Project web site: http://www.projectliberty.org/)

eC3

eC3 is an alliance of state and local governmental associations. Their mission is to advance the use of electronic commerce by governmental organizations. As part of this mission, they have published several white papers concerning identity management.

See: http://www.ec3.org/index.htm

SAFE-Biopharma Association

This identity management organization maintains and enforces the SAFE framework, which permits bio-pharmaceutical companies to digitally sign business-to-business and business-to-regulator transactions.

SAFE is a successfully operating federation which has solved a number of important cross-boundary issues including those of private-public sector and international boundaries. Based in the health industry, it is familiar with health issues and familiar to current industry participants. Representatives of SAFE participate in EAP.

See: http://www.safe-biopharma.org/

HSPD-12 / FIPS 201 / PIV

On August 17, 2004, President Bush issued Homeland Security Presidential Directive - 12 (HSPD-12). This directive called for a common identification standard for all federal employees and contractors. Given this directive, the National Institutes for Standards and Technology developed the Federal Information Processing Standards Publication 201 (FIPS 201), entitled Personal Identity Verification of Federal Employees and Contractors (PIV). This project will provide credentials to 10 to 12 million people at a relatively high level of verification and authentication and could be rolled out to many others through various extensions.

See: http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html

See Personal Identity Verification web site: http://csrc.nist.gov/piv-program/index.html

Real ID Act

The Real ID Act was passed in 2005 by Congress. The Act is intended to deter terrorism. Among other things, the law states that after May 11, 2008, no Federal agency may accept, for official purposes, a state driver's license as proof of identity unless that state's driver's license meets certain requirements defined by the Real ID Act. There is a debate as to whether the Act creates a national ID. The debate aside, unless the law is repealed, it will likely have a significant impact on how individuals in America manage their identities.

Real ID requires issuance of a machine readable credential based upon enhanced identity verification as well as improved security practice and technology. There will likely be many different ways to use the Real ID credentials as functions are built to extend the systems or use of the credentials and as States and/or the Federal Government extend the infrastructure. It is possible that one or more States could choose to issue further electronic credentials, PIN's, passwords, PKI certificates, etc., in conjunction with Real ID and/or join EAF or EAP to provide a channel for citizens to use the credentials across a broader range of our society.

Shibboleth

According to its web site, Shibboleth is "standards-based, open source middleware software which provides Web Single SignOn (SSO) across or within organizational boundaries." As part of the Internet2 project, Shibboleth "is developing architectures, policy structures, practical technologies, and an open source implementation to support inter-institutional sharing of web resources subject to access controls. In addition, Shibboleth will develop a policy framework that will allow inter-operation within the higher education community." The Shibboleth federation approach is being widely adopted in this country by educational institutions and internationally by government and private sector organizations. It is working to align its policies and practices to allow interoperability with EAF, EAP and others. Examples of initiatives that have adopted Shibboleth technology include: InCommon, EduCause, and LionShare. InCommon has set up InQueue as a learning environment for participating organizations.

See: http://shibboleth.internet2.edu/

Bylaws:
http://www.incommonfederation.org/docs/policies/InC_SCbylaws.html

Participant Operational Practices:
http://www.incommonfederation.org/docs/policies/incommonpop.html

Federation Operating Practices and Procedures:
http://www.incommonfederation.org/docs/policies/incommonfopp.html

Trust Service (WebTrust/SysTrust)

The American Institute of Certified Public Accountants initiated the WebTrust/SysTrust project. The AICPA's Trust Services are defined as "a set of professional assurance and advisory services based on a common framework (i.e., a core set of principles and criteria) to address the risks and opportunities of IT." Essentially, the project enables CPAs to offer a new service to clients: evaluating web sites that involve data transmission (e.g., personal information such as credit card numbers, birth date, health information, etc.). Web sites that meet the WebTrust/SysTrust requirements can post a "seal of approval" logo on their web sites.

See: http://www.webtrust.org/

JA-SIG Central Authentication Service (CAS)

CAS is a single sign on service offered by JA-SIG (Java Architectures). It is an open protocol that appears to be used primarily by the academic community. (It was originally created at Yale University.)

See: http://www.ja-sig.org/products/cas/

OATH

As described on its web site, OATH is "an industry-wide collaboration to develop an open reference architecture by leveraging existing open standards for the universal adoption of strong authentication." Its vision is to provide "a reference architecture for universal strong authentication across all users and all devices over all networks."

See: http://www.openauthentication.org/

American Health Information Community (AHIC) Confidentiality, Privacy & Security Work Group

The American Health Information Community (AHIC), a health IT advisory panel of the U.S. Department of Health and Human Services, in May 2006 established a cross-cutting work group on confidentiality, privacy and security. The Work Group's charge is to "make actionable confidentiality, privacy, and security recommendations to the Community on specific policies that best balance the needs between appropriate information protection and access to support, and accelerate the implementation of the consumer empowerment, chronic care, and electronic health record related breakthroughs."

See: http://www.hhs.gov/healthit/ahic/confidentiality

Healthcare Information Technology Standards Panel (HITSP)

HITSP will assist in the development of the U.S. Nationwide Health Information Network (NHIN) by selecting standards and publishing specifications to support use cases developed by AHIC and the Office of the National Coordinator for Health Information Technology (ONC). The Panel is sponsored by the American National Standards Institute (ANSI) in cooperation with strategic partners such as the Healthcare Information and Management Systems Society (HIMSS), the Advanced Technology Institute (ATI), and Booz Allen Hamilton.

See: http://www.hitsp.org

Center for Democracy and Technology (CDT)

In March 2007, the Center for Democracy and Technology released draft principles for identity in the Digital Age.

See: http://www.cdt.org/security/20070327idprinciples.pdf

PCI Security Standards Council

The PCI Security Standards Council is an open global forum for the ongoing development, enhancement, storage, dissemination, and implementation of security standards for account data protection. The PCI Security Standards Council's mission is to enhance payment account data security by fostering broad adoption of the PCI Security Standards. The organization was founded by American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International.

See: https://www.pcisecuritystandards.org/

Information Technology Association of America (ITAA)

ITAA provides global public policy, business networking, and national leadership to promote the continued rapid growth of the IT industry. The Association represents over 325 information technology companies. ITAA has an Identity Management Committee that was created to provide a forum for industry to work with federal, state, and global governments to develop best practices for the authentication and verification of identity, as well as to promote the use of technology to increase the security of our credentialing and access systems. Members include companies producing driver's licenses, national identity credentials, and other identity cards; managing federal, state, and local smart card and identity credentialing programs; providing biometric devices, radio frequency identification technologies, and middleware solutions; as well as performing background checks and other identity proofing services.

See: http://www.itaa.org

Appendix E: EAF/EAP Levels

The following is a very brief description of the E-Authentication Federation (EAF) among U.S. government agencies and its companion organization for private sector organizations, the E-Authentication Partnership (EAP). Please refer to the EAF home page (http://www.cio.gov/eauthentication/) for comprehensive documents and updates.

The National Institute for Standards and Technology (NIST) has documented EAF policies, standards, practices, and technology.

The EAF is designed to create a trust infrastructure for authenticating individuals who wish to connect to Internet-based services from federal agencies. The EAP, which licenses EAF standards, is a partnership attempting to enable interoperability for electronic authentication among public and private sector organizations. The EAF is further developed than the EAP, and for simplicity, we will refer to EAF for the rest of this discussion.

Credential Service Provider — An organization that offers one or more credential services (i.e., proofs and provides credential to individuals).
Relying Party — A person or agency that relies on the credentials issued by a Credential Service Provider.

Joining the EAF requires Credential Service Providers and Relying Parties to agree to use the components of the infrastructure, and to abide by the Business Rules and Operating Rules and comply with the requirements of the appropriate documents such as NIST SP 800-53 or NIST SP 800-63.

There are many technology, security, privacy, business, and operating requirements for all participating organizations covered by the suite of documents and components used to guide the implementation of the EAF. The following discussion will focus on those specific to identity proofing and credentials of individual users.

Relying parties within the EAF self-assess the risk associated with reliance upon e-authentication credentials.[13] Based upon this risk assessment, the relying party chooses which of four designated levels of authentication stringency will be required for accessing one or more of its online resources such as web sites, applications, or information.

Level 1 has no level-specific requirements for proofing or issuance (and thus does not have a section in the chart below). This level can be employed when the Relying Party does not have a need to ascertain the identity of the person accessing a resource. The consumer employs self-assertion, and she may employ a pseudonym. Due to the lack of identity proofing, the low level of security provided by Level 1 authentication is inappropriate for use in facilitating access to personal health information.

[13] See *Electronic Risk and Requirements Assessment (e-RA).* Accessed online on May 9, 2007, at: http://www.cio.gov/eauthentication/era.htm.

Proofing Requirements Under EAF

The table below[14] summarizes the requirements of Levels 2-4. Both in-person and remote identity proofing methods are permitted for Levels 2 and 3. Explicit requirements are specified for each scenario in Levels 2 and 3. Only in-person initial proofing is permitted at Level 4.

LEVEL 2		
	In-Person	**Remote**
Basis for issuing credentials	Possession of a valid current primary Government Photo-ID that contains applicant's picture and either address of record or nationality (e.g., driver's license or passport)	Possession of a valid Government ID (e.g., a driver's license or passport) number and a financial account number (e.g., checking account, savings account, loan, or credit card) with confirmation via records of either number.
Registration Authority Actions (Proofing)	Inspects Photo-ID, compares picture to applicant, records ID number, address, and DoB. If ID appears valid and photo matches, applicant then: a. If ID confirms address of record, authorizes or issues credentials and sends notice to address of record, or; b. If ID does not confirm address of record, issues credentials in a manner that confirms the address of record.	Inspects both ID number and account number supplied by applicant. Verifies information provided by applicant including ID number or account number through record checks either with the applicable agency or institution, or through credit bureaus or similar databases, and confirms that: name, DoB, address, other personal information in records are on balance consistent with the application and sufficient to identify a unique individual. Address confirmation and notification: a. Sends notice to an address of record confirmed in the records check or; b. Issues credentials in a manner that confirms the address of record supplied by the applicant; or c. Issues credentials in a manner that confirms the ability of the applicant to receive telephone communications or e-mail at number or e-mail address associated with the applicant in records.

[14] Table is adapted from *NIST Special Publication 800-63, Version 1.0.2, Electronic Authentication Guideline.* (April 2006). Accessed online on May 9, 2007, at: http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf.

LEVEL 3		
	In-Person	**Remote**
Basis for issuing credentials	Possession of verified current primary Government Photo-ID that contains applicant's picture and either address of record or nationality (e.g., driver's license or passport).	Possession of a valid Government ID (e.g., a driver's license or passport) number and a financial account number (e.g., checking account, savings account, loan, or credit card) with confirmation via records of both numbers.
Registration Authority Actions (Proofing)	Inspects Photo-ID and verifies via the issuing government agency or through credit bureaus or similar databases. Confirms that: name, DoB, address, and other personal information in record are consistent with the application. Compares picture to applicant, records ID number, address, and DoB. If ID is valid and photo matches applicant then: a. If ID confirms address of record, authorizes or issues credentials and sends notice to address of record, or; b. If ID does not confirm address of record, issues credentials in a manner that confirms address of record	Verifies information provided by applicant including ID number and account number through record checks, either with the applicable agency or institution, or through credit bureaus or similar databases, and confirms that: name, DoB, address, and other personal information in records are consistent with the application and sufficient to identify a unique individual. Address confirmation: a. Issues credentials in a manner that confirms the address of record supplied by the applicant; or b. Issues credentials in a manner that confirms the ability of the applicant to receive telephone communications at a number associated with the applicant in records, while recording the applicant's voice.

LEVEL 4		
	In-Person	**Remote**
Basis for issuing credentials	In person appearance and verification of two independent ID documents or accounts, meeting the requirements of Level 3 (in person and remote), one of which must be current primary Government Photo-ID that contains applicant's picture and either address of record or nationality (e.g., driver's license or passport), and a new recording of a biometric of the applicant at the time of application	Not applicable
Registration Authority Actions (Proofing)	• *Primary Photo-ID:* Inspects Photo-ID and verifies via the issuing government agency, compares picture to applicant, records ID number, address, and DoB. • *Secondary Government ID or financial account* a. Inspects Photo-ID and if apparently valid, compares picture to applicant, record ID number, address, and DoB, or; b. Verifies financial account number supplied by applicant through record checks or through credit bureaus or similar databases, and confirms that: name, DoB, address, other personal information in records are on balance consistent with the application and sufficient to identify a unique individual. • *Records Current Biometric Record* - a current biometric (e.g., photograph or fingerprints to ensure that applicant cannot repudiate application). • *Confirms Address* - Issues credentials in a manner that confirms address of record.	Not applicable

Ongoing Tokens Under EAF

The following tables describe the allowable uses of tokens under EAF levels 2-4. Table 2 shows the types of tokens that may be used at each authentication assurance level. Table 3 identifies the protections that are required at each level.

Table 2. Token Types Allowed at Each Assurance Level

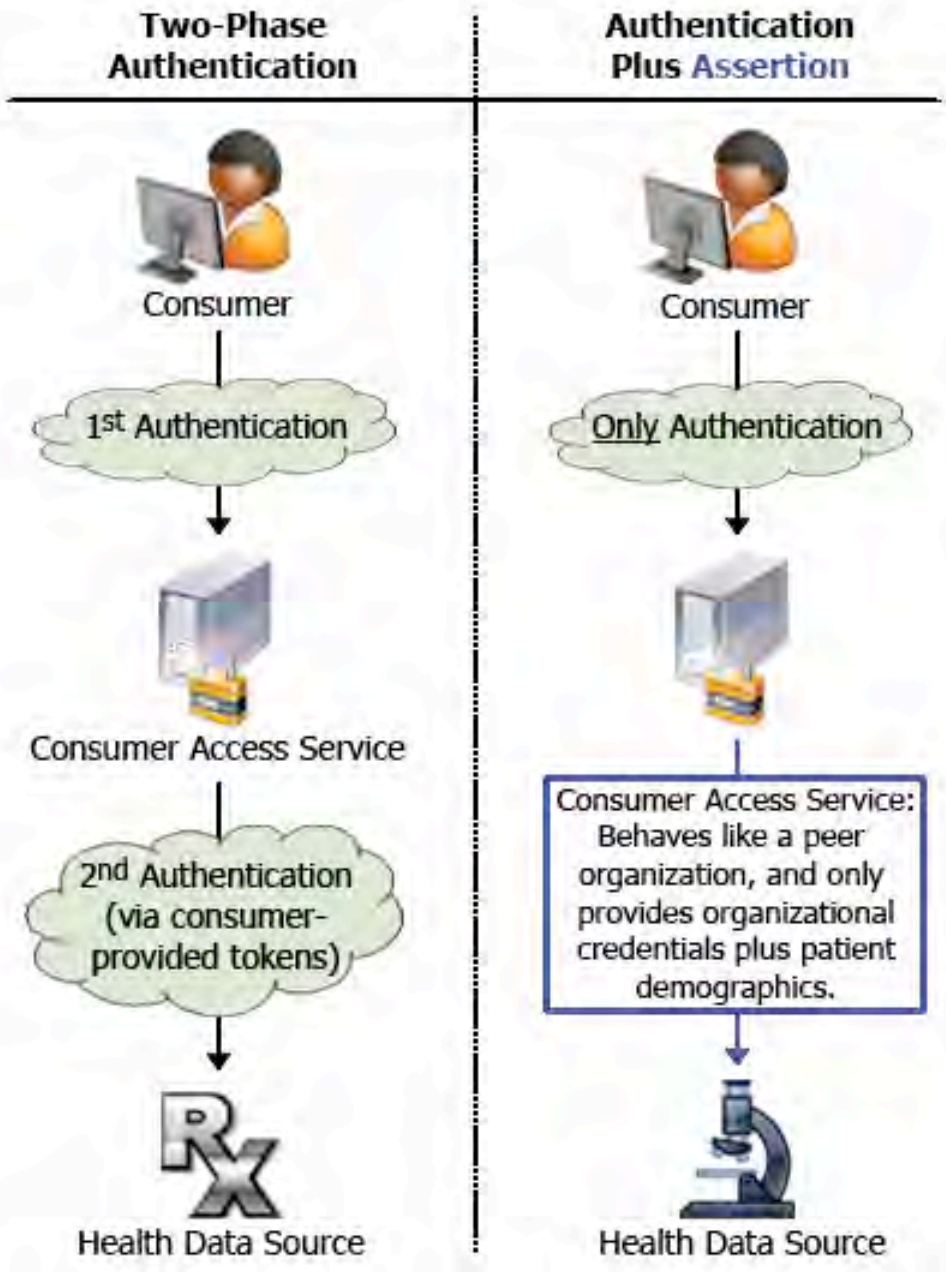
Token type	Level 1	Level 2	Level 3	Level 4
Hard crypto token	√	√	√	√
One-time password device	√	√	√	
Soft crypto token	√	√	√	
Passwords & PINs	√	√		

Table 3. Required Protections

Protect against	Level 1	Level 2	Level 3	Level 4
Online guessing	√	√	√	√
Replay	√	√	√	√
Eavesdropper		√	√	√
Verifier impersonation			√	√
Man-in-the-middle			√	√
Session hijacking				√

Appendix F: Two Models of Remote Authentication

There are at least two possible architectural solutions to the question of allowing a Health Data Source to accept a Consumer Access Services request for copies of a consumer's health data. First, the Health Data Source could re-authenticate the consumer. Collectively, we will call this repeated authentication process a **two-phase authentication** (not to be confused with two-factor authentication). Second, in lieu of re-authenticating the consumer, the remote data source could accept an identity assertion from the Consumer Access Service. Collectively, we will call this scenario **authentication plus assertion**. The diagram, text, and table below will elaborate on the differences between these two processes.



In **authentication plus assertion** (right hand model), the consumer only authenticates to the Consumer Access Service, which then transmits an assertion to the remote source indicating that the consumer is requesting data. In addition to this assertion, the Consumer Access Service passes along its own organizational credentials. The Consumer Access Service authenticates the consumer, but asserts to the remote data source that it is acting on the consumer's behalf by presenting the demographic information necessary to match the consumer to data held by the remote data source. Therefore, authentication plus assertion assumes that a data owner trusts another entity (i.e., the local application) to authenticate the consumer.

In **two-phase authentication** (left hand model), the consumer has two separate sets of authentication credentials and procedures. Both the Consumer Access Service and the remote data source maintain separate authentication information on the consumer. Each has gone through a process that initially proofs the consumer's identity, and each has an associated method for authenticating the consumer on an ongoing basis. The role of the Consumer Access Service is to both locally authenticate the consumer and to transmit the consumer's information that is required by the remote data source to perform its authentication process. In this second step, the Consumer Access Service acts only as a proxy.

Let's consider an example that illustrates **two-phase authentication**. Programs such as Quicken allow users to download data from remote sources (banks, brokerage firms, etc.) into the local application. When a user wishes to download data from her bank into her Quicken application, she must first authenticate locally (i.e., log into the Quicken software). Then, when she requests a data download, Quicken sends the login-name/password combination that corresponds to her bank's online banking service. (For convenience, the user has already stored her login-name and password within Quicken.) Thus, Quicken acts as the user's proxy during the remote data source authentication process. In the case that the local application is a web-based service, such as the Consumer Access Service, the local application can use mechanisms such as SAML to transmit the user's credentials.

This two-phase authentication model puts the burden of authentication on the consumer and the data sources. The individual must log in to multiple data sources before accessing data through the Consumer Access Service. Data gathering and authentication choices are handled by proximate data sources. Consumer access authentication choices are handled by the Consumer Access Service. This model is the safe deposit model — the consumer's authentication with the Consumer Access Service is unrelated to her authentication with the proximate data sources. There is also nothing specific to health care governing the collection of usernames and logins for remote services, increasing the risk.

However, having established that the consumer has authenticated both at the Consumer Access Service and at a data source, the Consumer Access Service and a data source could set up a business relationship such that all subsequent logins would be treated as the same person. This would make it possible to rely on the clinical data source's proofing mechanism, but the Consumer Access Service's authentication method. The weak link in this system is the Consumer Access Service authentication mechanism. The Consumer Access Service and the clinical data source would have to agree on the stringency of the Consumer Access Service authentication requirements, and have mechanisms for audit and redress.

In **authentication plus assertion**, the consumer only authenticates to the Consumer Access Service, which then transmits an assertion to the remote source indicating that the consumer is requesting data. In addition to this assertion, the Consumer Access Service passes along its own organizational credentials. The Consumer Access Service authenticates the consumer, but asserts to the remote data source that it is acting on the consumer's behalf by presenting the demographic information necessary to match the consumer to data held by the remote data source. Therefore, authentication plus assertion assumes that a data owner trusts another entity (i.e., the local application) to authenticate the consumer.

The table below compares these two processes based on a list of issues:

Authentication plus assertion does not scale well from the standpoint of industry since every local application must have agreements with all remote data sources. As the number of local applications and remote data sources increases, the total number of agreements rises exponentially. Therefore, this model is only practical if one of the following conditions is true:

1. There are a limited number of both data sources and local applications or intermediaries (i.e., if there were only a handful of Consumer Access Service providers).
2. There are a limited number of data sources.
3. There are a limited number of local applications or intermediaries.

Issue	Two-phase Authentication	Authentication plus Assertion
Ease of use for consumer		Advantage
Technical work for implementing authentication		Advantage
Number of proofing/token problems per remote access	2	1
Susceptibility to man-in-the-middle attacks		Advantage against browser hacks (but open to attacks between Consumer Access Service/data sources)
Susceptibility to error/abuse by human authorizer	Advantage	
Legal risk for remote data source	Advantage	
Scales well for establishing relationships from data source to Consumer Access Service	Advantage	
Cost to Consumer Access Service to implement	Low	High
Cost to individual data sources	High	Low

Authentication plus assertion requires data owners to be willing to delegate authentication to another entity. Unless a data source has developed appropriate legal agreements that cover mistakes made by delegates (e.g., releases of data to the wrong person), the data owner (and its insurance carrier) may be unwilling to delegate its authentication process to others.

It is not the purpose of our Work Group to endorse one model over another. We believe it important to note that both models will likely be offered in the marketplace for some time to come.

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.

CP1 CP2 CP3 CP4 CP5 CP6 CP7 CP8 CP9

CT1 CT2 **CT3** CT4 CT5 CT6 CT7

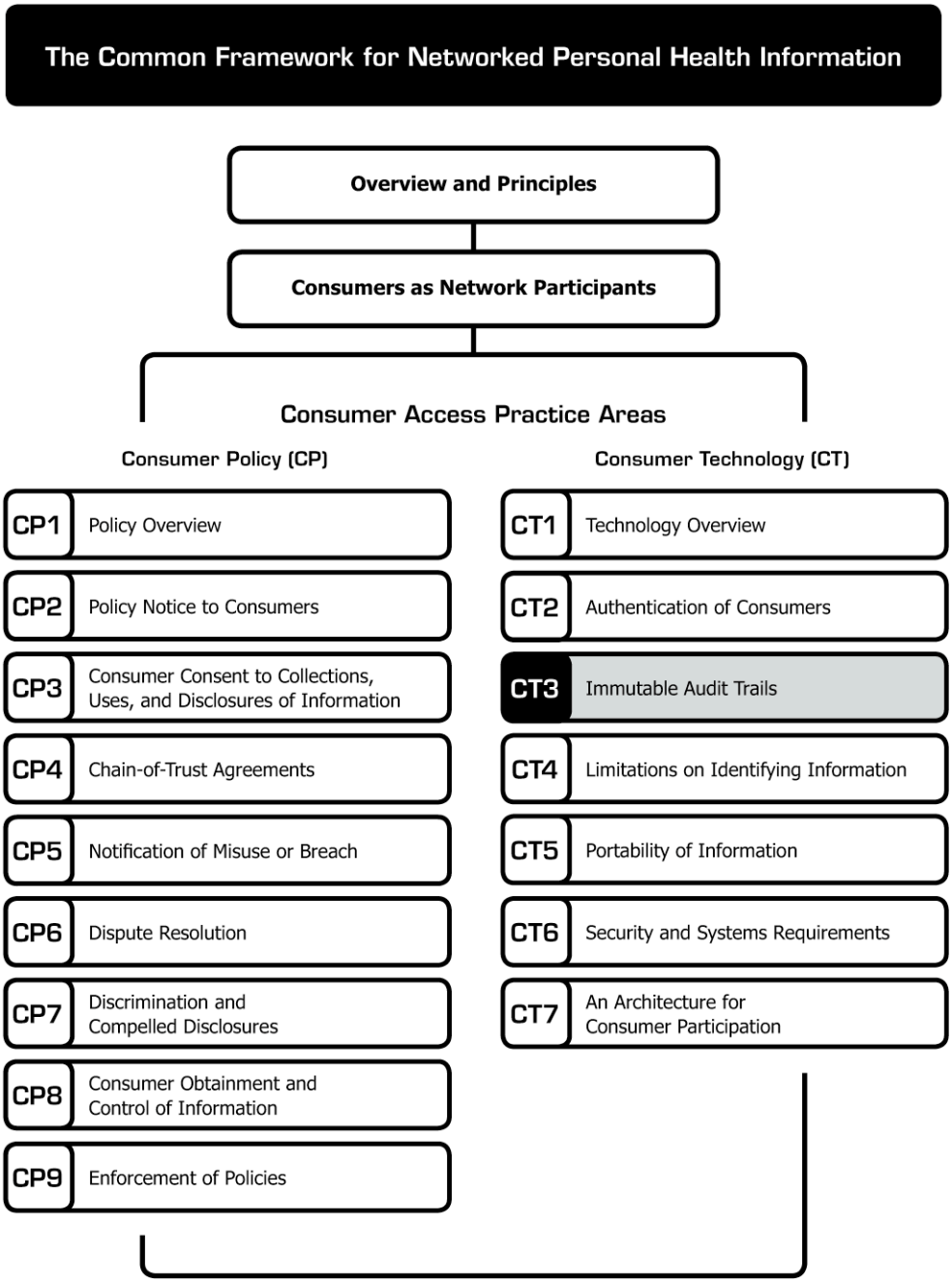
Immutable Audit Trails

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.*

CP1 CP2 CP3 CP4 CP5 CP6 CP7 CP8 CP9

CT1 CT2 CT3 **CT4** CT5 CT6 CT7

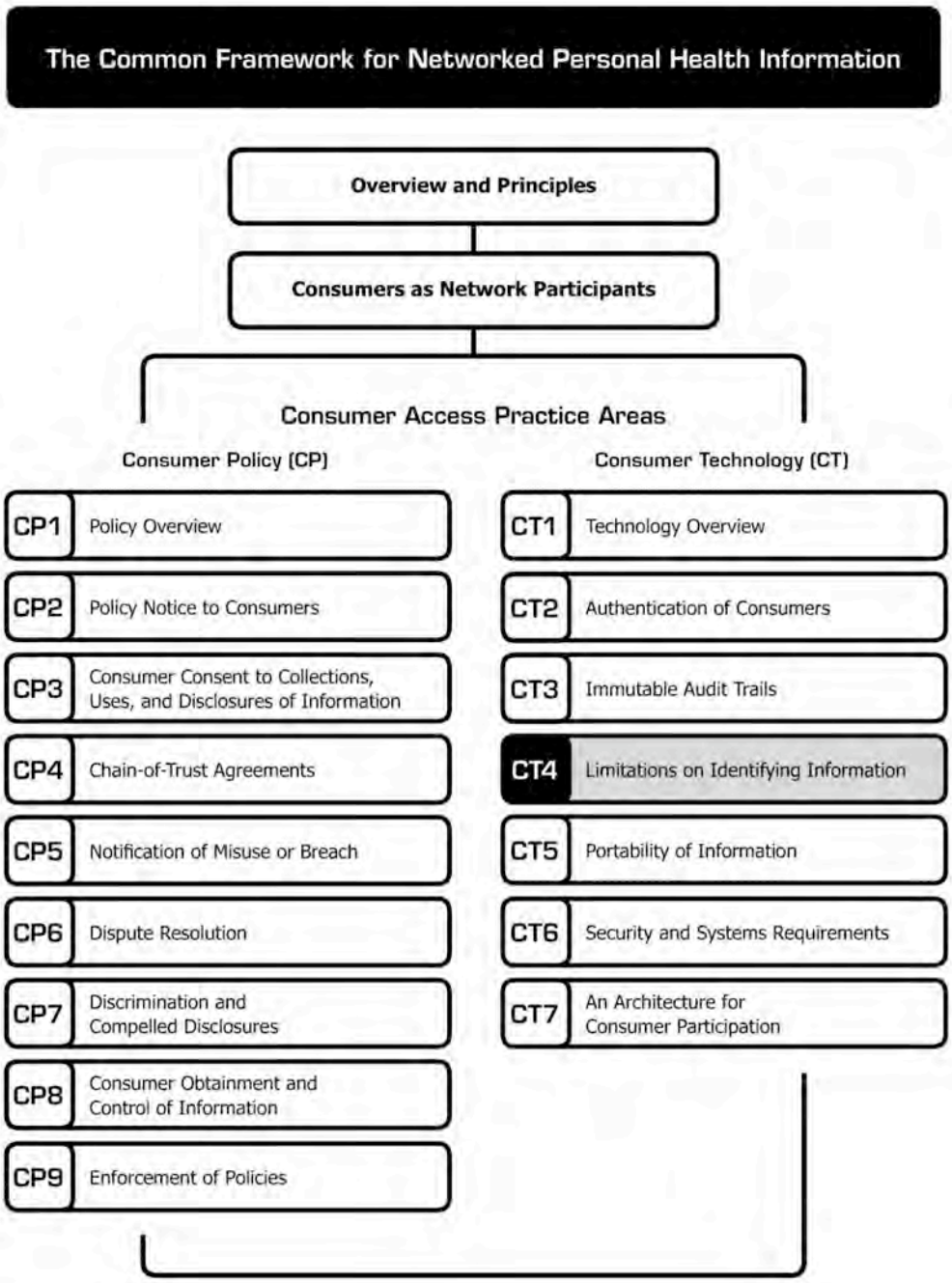
Limitations on Identifying Information

Limitations on Identifying 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:



Limitations on Identifying Information*

There are significant risks if business partners of Consumer Access Services are permitted to combine data with other databases to identify individuals or create a more complete profile of the consumer's health. Such practices have the potential to create unauthorized third party relationships of which the consumer may be completely unaware. Chain-of-trust agreements should prohibit this type of activity. (*See **CP4: Chain-of-Trust Agreements***.) In addition, Consumer Access Services can further protect consumers — as well as themselves — by ensuring that the identifying information they expose to partners is the minimal amount necessary. For example, in some cases, a Consumer Access Service could share a consumer's age, but not date of birth, with a third party because age is less potentially revealing of identity than a specific date of birth.

In the Internet Age, information is increasingly difficult to classify as "identified" or "de-identified," particularly as it is copied, exchanged, or recombined with other information. With rapidly evolving technologies and databases, it is more appropriate to describe a spectrum of "identifiability," rather than a binary classification of information as identifiable or not. The question could then become not whether de-identified information *might be* made re-identifiable, but rather *which entities* would be able to re-identify the information, *how much effort* they would have to expend, and *what limits* are placed on their doing so.

HIPAA Regulations (45 C.F.R. § 164.514) provide standards for de-identification, including a list of 18 "identifier" data elements that must be stripped out in order for a limited data set to qualify as "de-identified."[1]

The Privacy Rule also allows a second way to de-identify information by having a qualified statistician determine, using generally accepted statistical principles and methods, that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by the anticipated recipient to identify the subject of the information. The qualified statistician must document the methods and results of the analysis that justify such a determination.

This HIPAA regulation remains a reasonable industry standard for defining information as "de-identified" in many circumstances today. However, it may not be fully identity-protective in some contexts, such as when applied to very small subsets of populations, or with the ever-increasing amounts of "partially identifying information" gathered in electronic environments. (*See **Appendix A** for more on partially identifying information*.) This reality will necessitate frequent monitoring of risk by policymakers in both the public and private sectors.

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

2. Purpose specification

3. Collection limitation and data minimization

4. Use limitation

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.

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

[1] Accessed online on January 2, 2008, at the following URL: http://www.hhs.gov/ocr/combinedregtext.pdf.

Recommended Practice:

Consumer Access Services should limit disclosures of identifying data to only those data that are necessary to perform the specified function(s) that the recipient is authorized to perform.

Care should be taken to limit the release or exposure of information that can be directly or indirectly tied to an individual, including electronic identifiers such as IP address, cookies, and web beacons.

Any release of such indirectly or directly identifying information should be consistent with all nine **Connecting for Health** Privacy Principles and all of the Practice Areas of this Common Framework, particularly specification of purpose, limitation of use to only specified purpose, and no unauthorized combining of data to create a more complete profile of individuals.

Appendix A: "Partially Identifying Data"

In today's web environment, much of what consumers do is recorded and tracked by the sites they visit. Even when consumers are not logged in, various pieces of information are collected about them. These little bits of data are often not personally identifying at the time and point of collection. But in some cases, these bits of information can be combined with other bits of information to build a more complete profile of each user. When enough information is collected and combined, it can be used to identify individuals. Hence, we call this information "partially identifying." Examples include cookies, web beacons, and even search keywords.

For illustration, "persistent cookies" are little pieces of text deposited in the web browsers of consumers by the web sites they visit. In a similar way that a ticket from the dry cleaner lets the proprietor link the customer out front with the right clothes held in the back, cookies contain lookup information that lets a web site link a user to other information held about him in a database, such as preferences, search history, or checkout items for purchase on the site.

When the consumer returns to a web site at a later time, persistent cookies such as these can tell the web browser to display the user name, show whatever the user has specified to appear on the site's homepage, allow for access to previously entered search queries, or display information about items the user had previously added to a shopping cart.

When search engine companies collect user search query history "anonymously" (i.e., not tied to a specific user identity), the partially identifiable information the user provides can be identifying in and of itself if a consumer searches for information about her name, address, telephone number, and/or personal identifiers. When this information is combined with additional search queries that detail the user's interests, hobbies, health conditions, etc., a very personal picture can be elicited quite easily. For example, America Online in the summer of 2006 released 20 million "de-identified" search queries of more than 650,000 of its users with the intention to help researchers design better search engines. AOL initially claimed the search data had been made anonymous by replacing each search query's associated AOL username with a different unique user ID. But for those search queries that included identifying information along with personal interests, not only were some users' identities revealed, but also intimate details about their personal lives.

Another example of unintentional identification occurred as a result of an airline's practice of printing customers' frequent-flyer numbers on boarding passes in addition to names and seat numbers. An investigative reporter doing a story on identity theft retrieved a passenger's discarded ticket stub and used the information to purchase another ticket from the same airline (in this case from British Airways). In doing so, the reporter was granted access to additional pieces of the passenger's identity, including "passport number, date of birth, and nationality."

The above cases, in which partially identifying information is used by external parties to identify an individual, occurred outside of contractual agreements. However, they do illustrate how the identifiability of information can change over time.

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.*

CP1 CP2 CP3 CP4 CP5 CP6 CP7 CP8 CP9

CT1 CT2 CT3 CT4 CT5 CT6 CT7

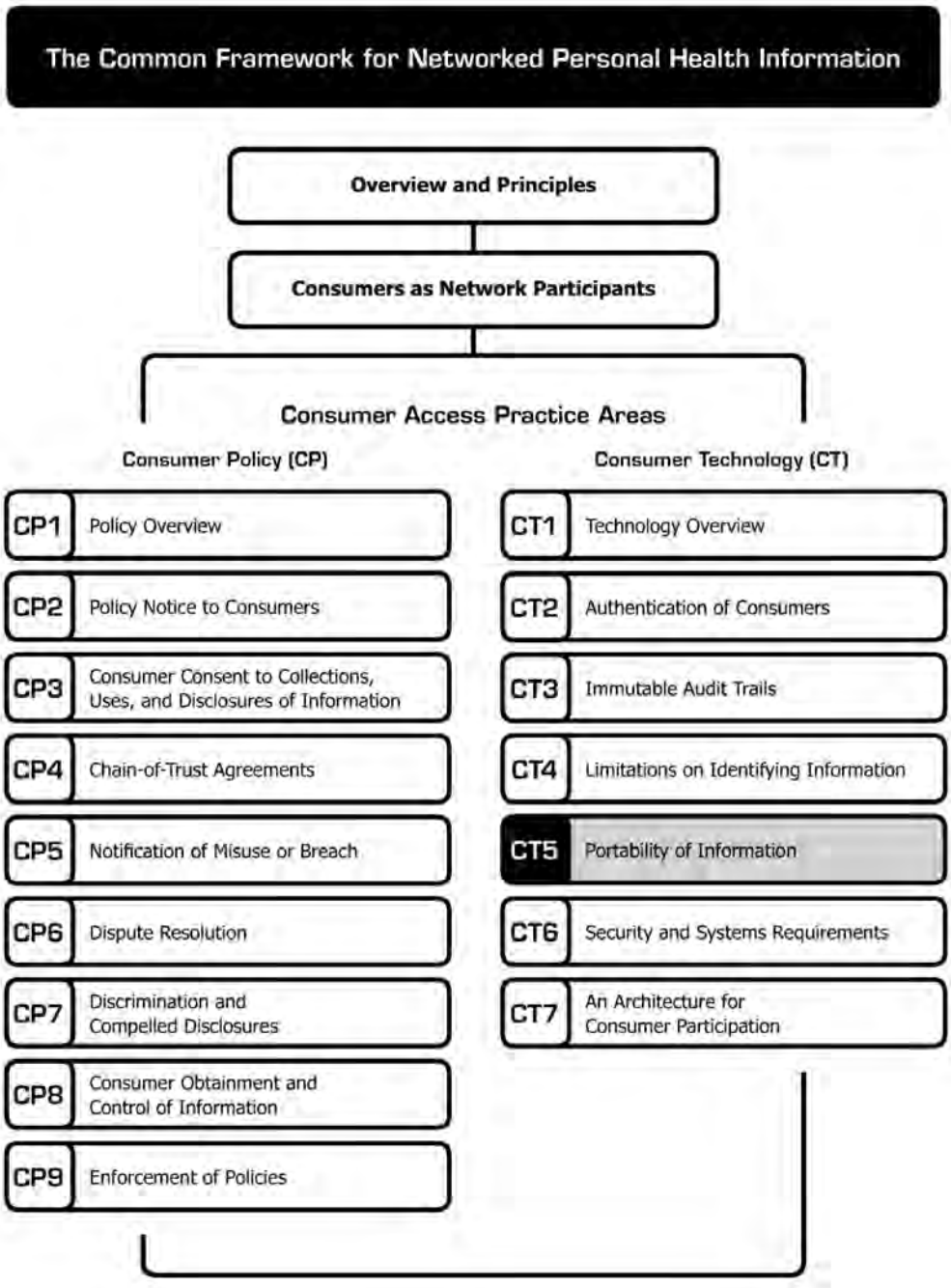
Portability of Information

Portability 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:



Portability of Information*

Purpose: Over time, individuals move, change jobs, change providers, develop health conditions, require new services, etc. We envision a competitive market of Consumer Access Services and networked PHRs that meets the needs of many different populations at various stages of their lives. For the overall health of the emerging industry, consumers should be able to make their personally identifiable information available to any and all applications to best meet their needs.

We recommend that the industry work on standardized permissions and formats for the exporting of data from one Consumer Access Service to another upon consumer request.

Export of Data to the Consumer

Consumer Access Services should provide mechanisms for the consumer to export information from her account in standard formats. The ideal state is that consumers would have a menu of output formats that are both human-usable and machine-readable. As health data subsets become standardized in the EHR and PHR industries, Consumer Access Services should support such standards. Ideally, Consumer Access Services would provide a mechanism for the consumer to export all data in the account in a human-intelligible format into standard software such as a spreadsheet or text file. Print capability is a reasonable minimum requirement. Once the consumer assumes full control of the copies of data (e.g., stores them on his computer hard drive), it is the consumer's sole responsibility to protect them.

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

5. Individual participation and control

* "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.

Recommended Practice:

Consumer Access Services should provide an easy-to-use mechanism for consumers to export information in their accounts for personal use. Such mechanisms should:

- Provide information in human-readable form.
- Include audit trail information for data entries (time-, date-, and source-stamping of each diagnosis, for example). *(See **CT3: Immutable Audit Trails.**)*
- Include a printer-friendly format.
- Conform to industry standards for health data subsets as they become available and broadly implemented.
- Enable data to be exported into industry standard software, such as spreadsheets, PDFs, or text files.

Export and Import of Data Among Consumer Access Services and PHRs

The ideal future state is for consumers, according to their changing needs and wishes, to be able to transfer their information from PHR service or application to another PHR service or application. Such electronic interoperability is not a market reality today. However, Consumer Access Services should support interoperable data exchange protocols and data standards as they become available and market-tested.

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

Recommended Practice:

Consumer Access Services should support industry-standard data sets for exchanging patient health information as they become available and broadly implemented. Consumer Access Services should collaborate to create a standard messaging envelope to export and import information upon the consumer's authorization.

In the absence of full data exchange interoperability, Consumer Access Services may provide consumers with storage options for documents gathered from past Consumer Access Services or other Health Data Sources. For example, a consumer could export information from one Consumer Access Service into a standard software format such as PDF and store it on her desktop, then upload those PDF documents into a secure account at a new Consumer Access Service.

*(For related recommendations, **see CP8: Consumer Obtainment and Control of Information** Area 5: Expunging of Information and Area 6: Termination of Account.*

*See also **CT3: Immutable Audit Trails** for recommendations on tracking export and import of data.)*

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.*

CP1 CP2 CP3 CP4 CP5 CP6 CP7 CP8 CP9

CT1 CT2 CT3 CT4 CT5 **CT6** CT7

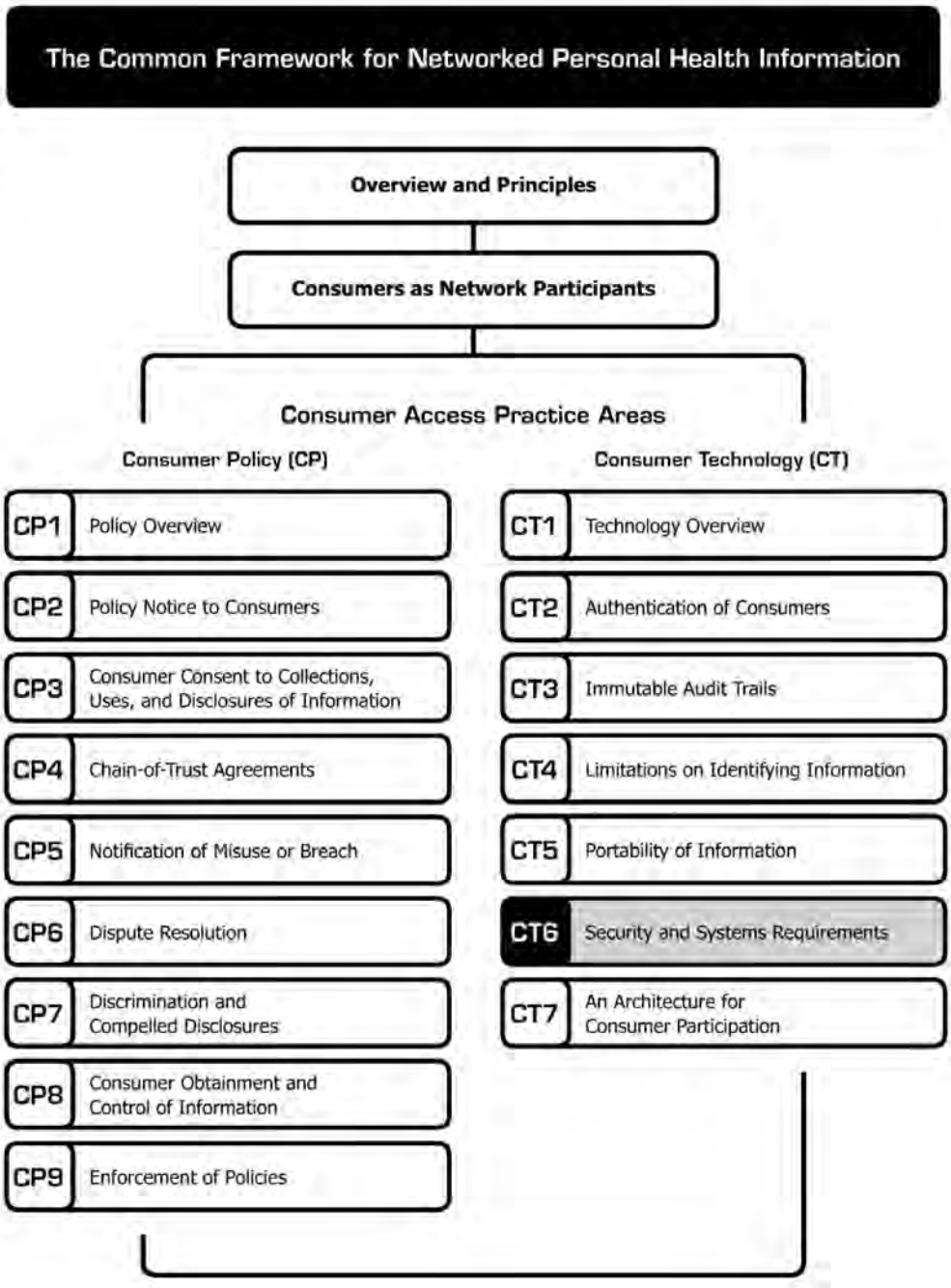
Security and Systems Requirements

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.*

CP1 CP2 CP3 CP4 CP5 CP6 CP7 CP8 CP9

CT1 CT2 CT3 CT4 CT5 CT6 **CT7**

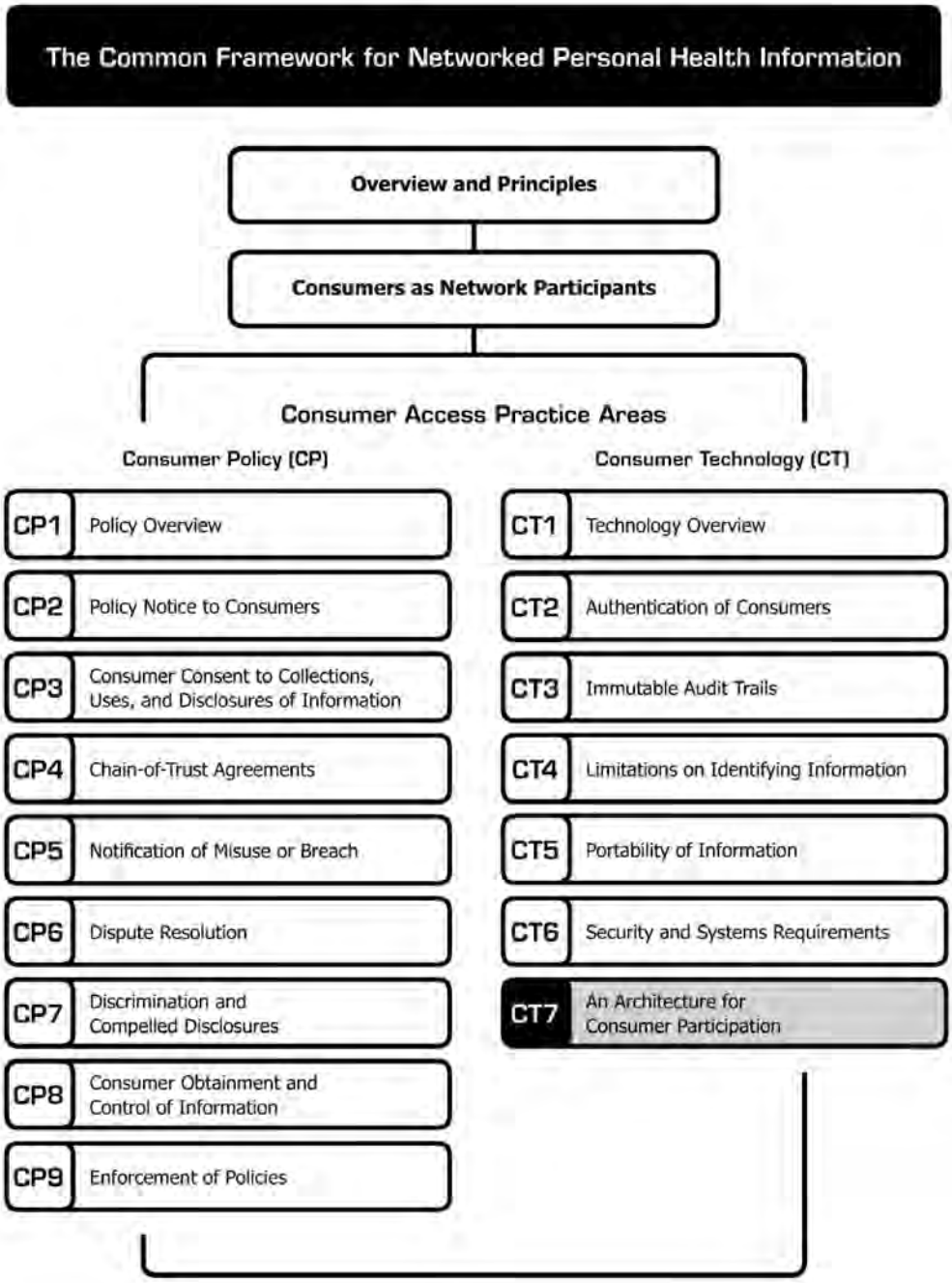
An Architecture for Consumer Participation

An Architecture for Consumer Participation

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:



An Architecture for Consumer Participation*

Purpose: This paper considers how consumer access to personal health information fits within the **Connecting for Health** Common Framework approach to a Nationwide Health Information Network (NHIN). To begin, there are two critical considerations:

1. In our vision, the NHIN is not a new network, but rather a way of using the existing Internet for private and secure health information exchange based on a set of common policies and practices.
2. Many different types of health information networks can be connected via the Internet, including local health information exchanges (HIEs), provider systems, data clearinghouses, and a rich variety of consumer-oriented applications.

The first set of **Connecting for Health** Common Framework resources, released in April 2006, was designed to enable interoperable exchange of patient data *among clinicians*. It is a substantial challenge to add consumers to the exchange. From the policy standpoint, it is necessary to develop an adequate set of information-sharing policies to which both consumers and institutional data custodians can agree. On the technical side, a network architecture must be consistent with fair information practices, and scalable and adaptable to the many combinations of relationships that consumers have with various health care entities. These technical and policy challenges must be addressed in tandem.

* **Connecting for Health** thanks Josh Lemieux, Markle Foundation; Clay Shirky, New York University Graduate Interactive Telecommunications Program; and David Lansky, PhD, for drafting this paper.

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.

Common Framework Technical Principles

The Common Framework prescribes several technical principles upon which health information exchange networks should be based. We summarize them below:

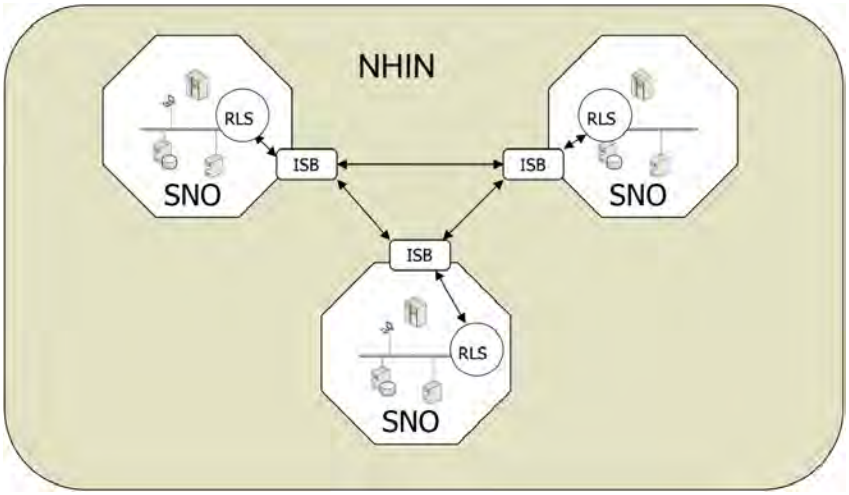
- **Make it "thin":** Data exchange networks should impose the minimal requirements for storing and transmitting health data, leaving as much processing as possible to applications at the edges of the network.
- **No requirement of a national health ID:** We argue that a national health identifier is neither likely nor necessary.
- **Avoid "rip and replace":** The health care industry has already invested heavily in technology. The network should take advantage of the technology currently in use, not require its replacement.
- **Separate applications from the network:** The roles of the network and of applications should be distinct. The purpose of the network is simply to transfer data. All other data-related functions should reside at the application level. This architecture provides for a stable infrastructure upon which application developers may build innovative functions.

- **Local control of data:** This principle holds that data not need be centralized in a new database in order for it to be shared among authorized parties, and that data may be shared directly (i.e., point to point) among authorized parties according to a consumer's needs and wishes. The primary responsibility to maintain accuracy of information should reside with the organization that captured it. However, as we discuss below, nothing in this principle should prevent a consumer from aggregating copies of her health information from multiple sources into a centralized service, if that is what the consumer wants.
- **Federation:** A federation of network members based on mutual agreements is necessary given the complexities of a decentralized network.
- **Flexibility:** The network should be designed such that it can scale and adapt over time and allow participation by a wide variety of network members.
- **Security and privacy:** Privacy protection and security should be top priorities that guide the design and development of the network.
- **Accuracy:** All reasonable efforts should be made to identify people accurately and maintain accurate records. There should be well-documented methods for identifying and correcting inaccurate information.

Connecting for Health put these principles into practice in a three-region prototype documented in previous Common Framework technical and policy papers. This paper adds to a compendium of policy resources for interoperable electronic health information exchanges. Those resources consist of:

- An overarching "architecture" for privacy based on nine interdependent principles.
- Model privacy policies and procedures.
- Notification and consent policies.
- Policies for correctly matching patients with their records.
- Policies for authentication of system users.
- Patient information access rights summary based on the Health Information Portability and Accountability Act (HIPAA).
- Policies for audit logs.
- Policies for breaches of confidential health information.[§]

The fundamental design elements of the **Connecting for Health** approach to network architecture would not be changed by granting consumers access to the network. In fact, consumer access has always been a design principle of the work. Below we review some of the key architectural concepts described more fully in prior Common Framework reports.



[§] The **Connecting for Health** Common Framework Policy and Technical Resources are available at: http://www.connectingforhealth.org/commonframework/overview.html.

- **Nationwide Health Information Network (NHIN):** As its name implies, the NHIN is an overarching network that connects exchange networks within the nation. Thus, it is envisioned as a network of networks.
- **Regional Health Information Organization (RHIO):** The current trend in health information exchange is to build provider-centric, regionalized networks. These networks are usually referred to as RHIOs. A functioning RHIO would connect multiple provider institutions in a region, such as a state or county.
- **Sub-Network Organization (SNO):** A Sub-Network Organization is a business structure comprised of entities that agree to share personal health information in accordance with a minimum set of technical and policy requirements embodied in the Common Framework. A SNO may be organized on a geographic basis (i.e., a RHIO) or in support of other business relationships that are not determined by location. For instance, the Veterans Administration (VA) has a network of hospitals and clinics that exchange health information on a nationwide level. Both RHIOs and non-regional networks like the VA would be sub-networks of the NHIN. Thus, we prefer the term "SNO" because it is a more inclusive term than RHIO.
- **Record Locator Service (RLS):** As its name implies, the RLS is a service that queries the locations of patient records within a SNO. Each SNO has its own RLS. The purpose of an RLS is best described by an example. A physician or other health care professional may wish to retrieve data on a patient from other institutions that the patient has visited. The physician would send a query to the RLS, which returns a list of record locations, but not the data itself. Thus, the RLS might inform the doctor that her patient has medical records at institutions X, Y, and Z. The contents of those records are not revealed by the RLS. Retrieval of data contained in an identified record is a separate process that occurs directly between the requesting physician and the institution that stores the record.
- **Inter-SNO Bridge (ISB):** A physician might want to search for records outside his SNO. Thus, he would send a query to the RLS of another SNO. The ISB is the conduit through which these queries and responses flow. Each SNO would have an ISB, which would be its single gateway for channeling all requests and responses from other SNOs.

In summary, the Common Framework architectural vision is a network of networks (one NHIN made up of many SNOs). Each SNO uses an RLS to locate the consumer's records and an ISB to talk to other SNOs. Institutions that want to share information across the network must be members of a SNO, comply with Common Framework policies, maintain an RLS or equivalent service, and build an ISB.

As noted in ***CT1: Technology Overview***, many important pieces of the consumer's record are already held in digital format. The custodians of this information include:

- Health insurance plans (both private and public).
- Pharmacy services and clearinghouses.
- Nationwide laboratory services.
- Self-insured employers' data warehouse services.
- Large, integrated delivery networks.
- And, to a lesser extent, some small hospitals and smaller-practice EHRs.

How Consumers Could Be Networked Via the Common Framework

Most currently available PHRs either rely on existing data silos (i.e., patient portals offering access to non-interoperable health records) or create new silos (i.e., consumer-populated, non-interoperable records). Potential large-scale benefits of PHRs are unlikely to materialize if these applications remain dependent on limited data sources.[1] For PHRs to become more universally useful to consumers, they must provide a convenient and secure means of connecting to personal data and interactive services from multiple sources, *and* they must provide a convenient and secure means of moving the data out of the PHR as well, in whole or in part.

A number of architectural approaches could permit consumers to deliver information from disparate data sources into a PHR and vice versa. At one end of the spectrum, the PHR could rely entirely on a **centralized database of personal health information**. A master database at the center of the network would aggregate data from other health information systems before the information becomes accessible in the PHR. Theoretically, the consumer could then have access via one interface to the central data repository, with potentially greater efficiencies than could be provided by queries across a distributed network. The primary problems with this centralized approach are:

1. **Data management:** Copying all personal health data to a single database, and keeping it all up to date, is impractical at population scale given the vast amounts of data that exist across systems.
2. **Data quality:** Sending all data to a central database may magnify data quality problems (although such an effort may also reveal data problems). The centralized repository model would make error checking and data reconciliation difficult compared to a model that keeps personal health information close to the entity that creates it and knows the patient. Organizations closest to the consumer are in the best position to validate, adjudicate, or update the consumer's data.
3. **Business case:** It is implausible that any one entity can emerge to garner the trust of all health care systems and all consumers in the fragmented U.S. health care environment. A single, central database would raise questions central to trust such as who controls the data, who governs the process, what secondary uses and resale of data will be allowed, etc. A single source of control for the database would risk the shortcomings of monopolies in general: low innovation, poor customer service, and higher prices. It also limits the power of the network to grow organically and incrementally.
4. **Security and privacy:** While breaches are a concern for all information holders, a centralized model poses significant risk to privacy since a single security breach could lead to a catastrophic data leak.

Centralized systems can provide valuable efficiencies and controls, and may be very appropriate at various network nodes, which should have flexibility with regard to data-storage solutions for the information that they each hold. If centralization is the only model by which health information can be shared across disparate entities, however, there is a high risk that many entities will not participate.

The polar opposite of the centralized architecture is an **entirely peer-to-peer network**. Under this model, a consumer would have to create and manage separate data streams between her PHR and each system that holds her data. The primary problems with the completely decentralized approach are in many ways the mirror image of the problems of absolute centralization:

[1] National Committee on Vital and Health Statistics [homepage on the Internet]. Washington: Department of Health and Human Services; [updated 2005 September 9; cited 2006 May 8]. September 9, 2005 Letter to Secretary Leavitt on Personal Health Record (PHR) Systems; [about 16 screens]. Available at: http://www.ncvhs.hhs.gov/050909lt.htm.

1. **Data management:** If each consumer is expected to aggregate her data, she will become both her own registrar and her own system administrator. This burden will be too much for the majority of consumers.
2. **Data quality:** Clinical data comes in both highly structured and very unstructured forms. The consumer would be responsible for managing these disparate forms of data — again, a task too challenging for most consumers.
3. **Business case:** Each person would pay for (or choose a sponsorship model for) a PHR, but the system would be highly fragmented and create few economies of scale.
4. **Security and privacy:** The security risk would be multiplied across many servers with varying levels of technical support and policy compliance. However, the breach of any given source of data would be more limited, reducing the potential for catastrophic data disclosures.

The pure point-to-point approach would place too much burden on the consumer to establish electronic transaction relationships with all of her health care services. It also would be cumbersome and pose high risks for each of the consumer's data sources, given the current lack of standards for clinical information or of a trusted mechanism to authenticate each consumer. Further, providers would be less likely to access and use the consumer's data if they were confronted with a hodgepodge of information aggregated from a series of unstructured point-to-point transactions.

How Could Consumers Aggregate Their Data?

Creation of centralized data repositories should not be an architectural requirement for data sharing, however, data aggregation at the level of the consumer could be very beneficial. How, then, can the individual aggregate her health data without relying upon a single repository at the center of the network or learning to manage a completely peer-to-peer model?

Any practical strategy for networking PHRs must avoid the negative consequences of these two extremes while satisfying the consumer's need to access and control her information.

The Common Framework vision of a federated, decentralized network of SNOs was created to meet this core requirement. Under the Common Framework, authorized clinicians are able to query the network (e.g., request an index of the locations of a patient's records) on the basis of their organization's membership in a SNO. To establish a chain of trust, the participating SNOs must have common understandings and expectations, such as how to authenticate and authorize clinicians to use the network and how to log their actions.

Consumers also need a chain of trust to interconnect across networks. Yet they represent a greater challenge than clinicians for authentication, authorization, liability, and security. There is no commonly accepted set of practices today to provide credentials to consumers for health information exchange across different systems and data repositories. It is reasonable to expect that consumer applications could become more easily "networked" if such a set of common practices existed — that is, if some type of enforceable arrangement required all participants to operate under a common set of policies and agreements to mitigate risks such as misidentification or identity theft.

In the **Connecting for Health** model, a network of interconnected SNOs is viewed as the most flexible and practical means to untether applications from data silos, as well as to enforce a common set of rules among participants. To integrate PHRs into the NHIN, we assume that the same model for connecting users — a chain of trust, brokered by an ISB that can talk to other entities in the system — must be available to patients and consumers. This paper considers the functions and requirements of an entity that provides consumers with access to the nationwide network of SNOs.

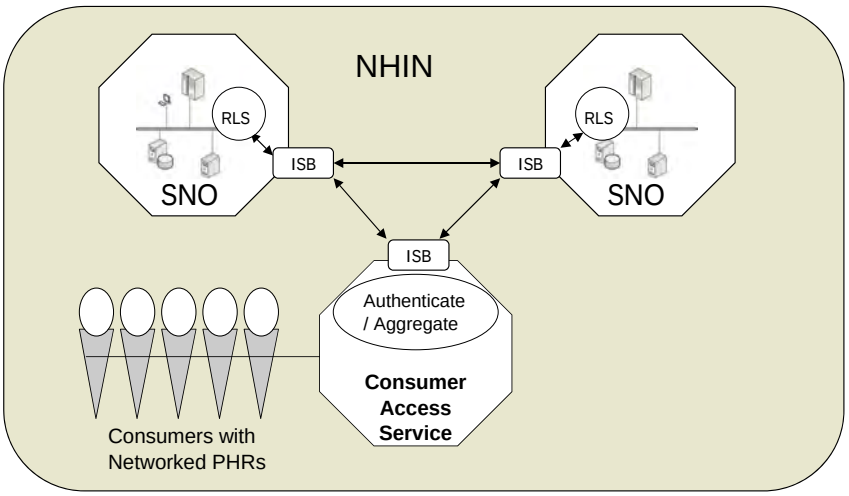
Consumer Access Services Could Act as Intermediaries

We start with three assumptions about how consumers could gain access to their data in the future. The first is that there will be services acting on the consumers' behalf as aggregators of personal health information. Other kinds of networked services with many sources of data, from e-mail to online bill paying to airline booking sites, aggregate data on behalf of the user. It may become technically possible for the consumer to access her health data (via a personal computer) directly from the hospitals, labs, and other organizations that hold it. However, even in such a scenario, many services will arise to hold and manage the data on the consumer's behalf. Issues of backup, remote access, and economies of scale are in fact already driving the creation of these sorts of services. (Some models may offer storage services of all of the consumer's data; others may emerge simply as gateways for access without actually storing the data. Ideally, consumers would choose which aggregation model best serves them.)

The second assumption is that there will be services that issue identity and authentication credentials to the consumer and pass those credentials or proof of authentication to other organizations in the NHIN, on the consumer's behalf. Today, we have no generally accepted methods or policies for initially proving the identity of each individual for the issuance of online credentials based on that identification, nor for the initial and repeated authentication of that individual's identity in an online environment. In a nationwide health information network, those who hold personal health data will need to be confident that the person to whom they transmit data is indeed who she claims to be. Common, reliable policies for initial proofing and repeated verification of identity will be essential functions of these intermediary services. (Although a complex set of issues surround identity, authentication, and authorization, we will group all of these issues under the label “authentication” for the rest of this document.)

Given the high cost of the initial consumer identification and the low cost of the subsequent authentications, economies of scale will drive the creation and growth of these functions. These intermediary services would be contractually obligated to comply with the rules governing participation in the network. Likewise, they would be expected to enforce those rules in the event of any violation by one of their authorized users (and to successfully exclude unauthorized users). By the same logic, the entities that issue identity credentials to individual consumers must have the organizational standing to enforce nationwide policies within their network. *(See **CT2: Authentication of Consumers**.)*

Third, we assume that the aggregation and authentication functions will be combined. While aggregation and authentication could be offered separately, the economic logic driving the creation of the services will also drive their combination. As a result, competing services would act as proxies for many consumers, potentially millions at a time, holding both their authentication tokens and their data. These authentication/aggregation service providers would not necessarily be covered entities under HIPAA. We call them “**Consumer Access Services.**” We will also assume that the interaction between Consumer Access Services and other entities in the NHIN will use the service-oriented architecture of the Common Framework, including both SOAP messages and message brokering by Inter-SNO Bridges.



Following the diagram above, such a combined authenticating and aggregating service would perform key NHIN functions including, at a minimum, authenticating individual users, providing an ISB interface to bridge between those users and the rest of the NHIN, and aggregating information into PHRs on those users' behalf.

A number of entities may be interested in offering these combined services to enable consumer access to the NHIN, including the following examples:

- **Provider organizations** could strengthen their role as primary care providers and care coordinators by accessing all of a patient's data when authorized and playing the role of interpreter and coach.
- **Health insurance plans and government programs** (e.g., Medicare, Medicaid, VA) could apply their data analytic- and decision support-capabilities to the clinically rich patient data available across the network and compete on their ability to deploy beneficial interventions based on that analytic intelligence.
- **Pharmacy services** (i.e., pharmacy benefit managers, retail pharmacies, clearinghouses) could offer new services to attract consumers.
- **Application vendors** could benefit from a more efficient marketing and distribution environment by offering their products to a range of Consumer Access Service suppliers with large populations of consumers.
- **Affinity and patient advocacy groups** could create their own intermediary services to help members select and use appropriate products, while using aggregate data as a platform for improving health and advocating for shared concerns.
- **Employers** could steer employees toward Consumer Access Services that allow secure access to personal health information and other benefits.
- **Web portals and other non-traditional health care players** could enter the health care space, both leveraging their brand credibility and gaining appropriate access to data that the consumer wants them to have without negotiating separate access agreements with each trading partner.
- **Regional Health Information Organizations (RHIOs)** could offer services to connect consumers.

Connecting for Health wishes to enable consumers to aggregate and manage their health care data while protecting them against the misuse or loss of personal data.

Public policy must make it possible for each person to access personal health information regardless of where it was originally acquired and where it is now maintained. In solving a problem like authentication, the NHIN needs to make sure that every American has an opportunity to gain the necessary credentials and take advantage of the information channels that exist, without being subservient to any particular gatekeeper.

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.*