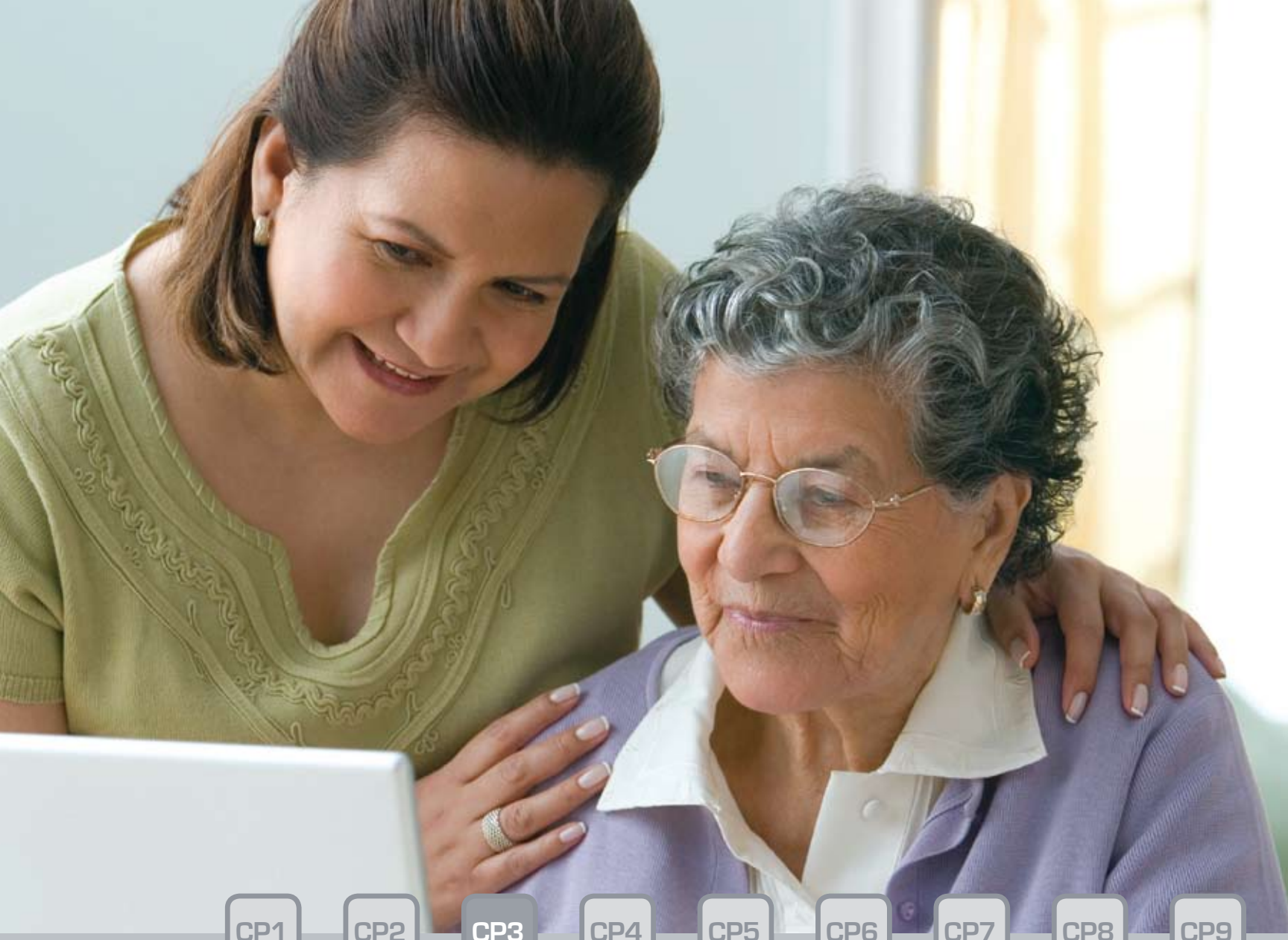


CP1 CP2 **CP3** CP4 CP5 CP6 CP7 CP8 CP9

CT1 CT2 CT3 CT4 CT5 CT6 CT7

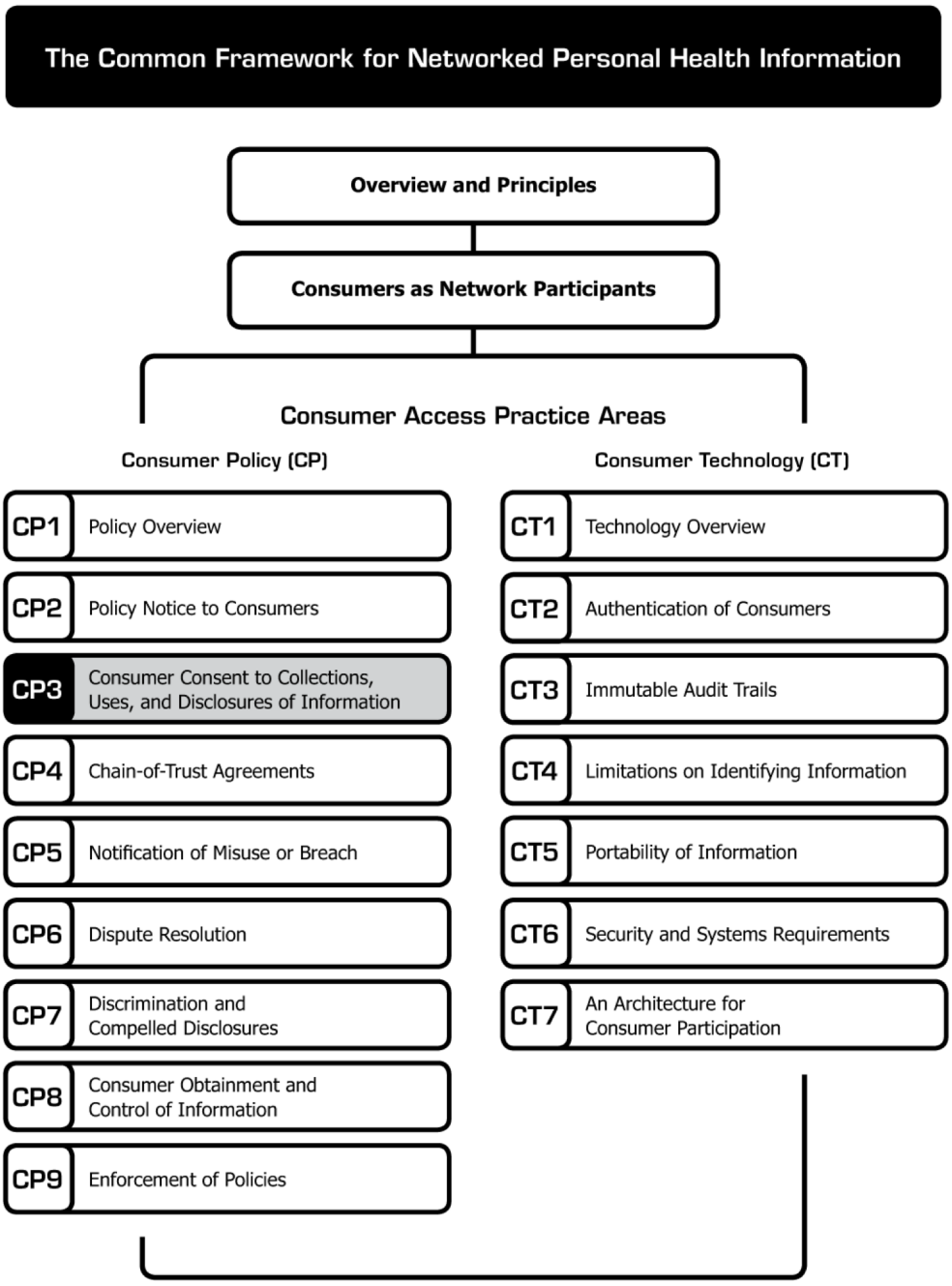
Consumer Consent to Collections, Uses, and Disclosures of Information

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.*