Connecting for Health Common Framework for Health Information Exchange Networked Personal Health Information

Carol C Diamond MD MPH
Markle Foundation

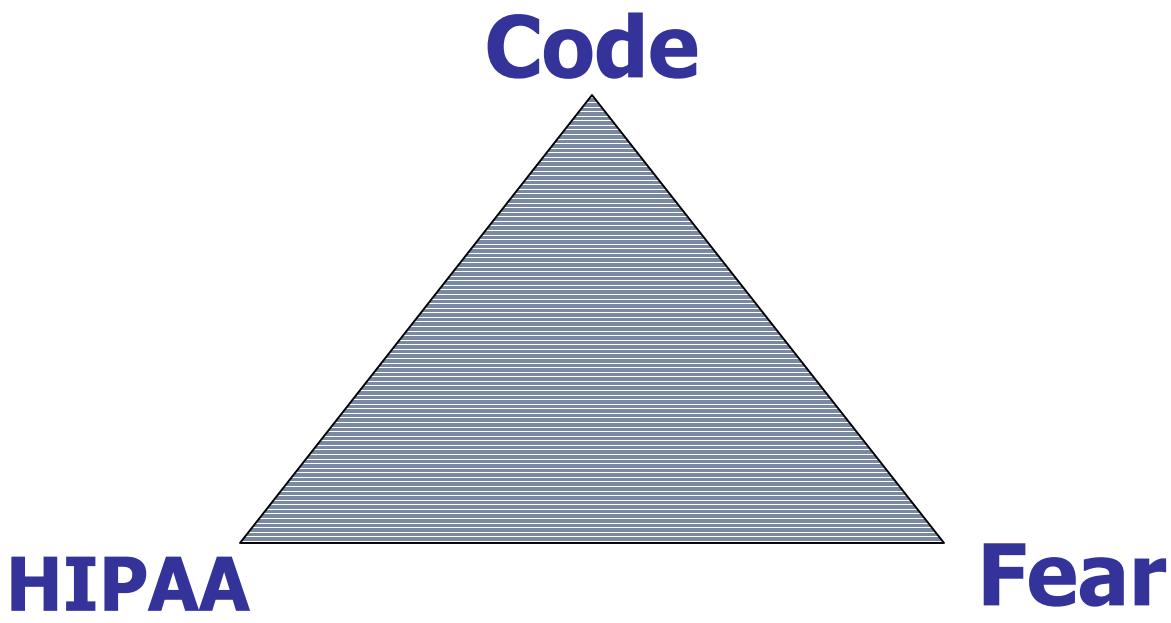
HIPAA Summit
August 20, 2008

Establishing TRUST and INNOVATION in HEALTHCARE

Code, HIPAA and Fear

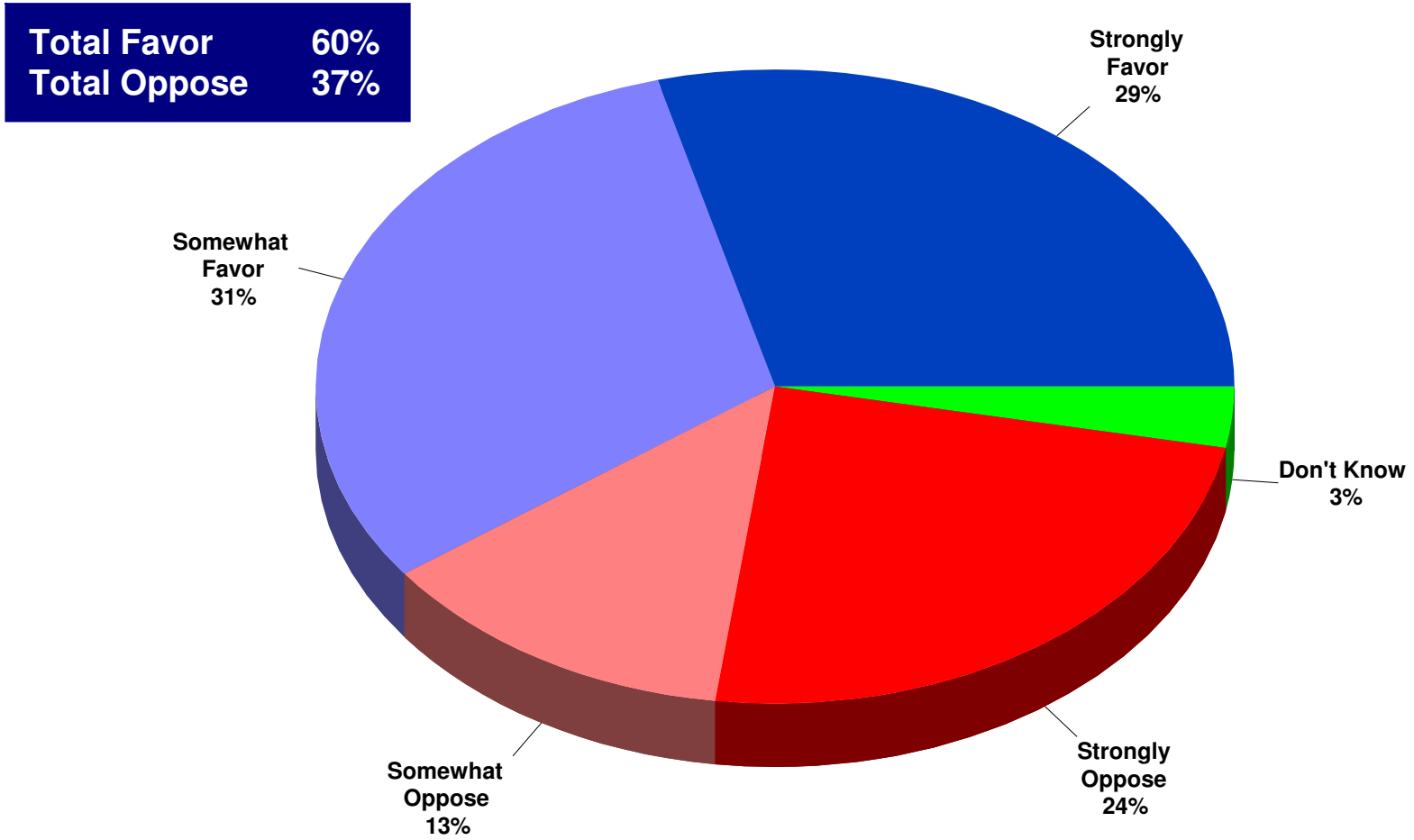
21st Century Attributes of Trust

The Current Paradigm



What do we know from public opinion surveys and focus groups?

Overall six out of ten Americans say they would favor the creation of a secure online “personal health record” service for their own use.



Now, overall, would you favor or oppose the creation of this type of secure online "personal health record" service?

There is also a strong interest among consumers in using health information technology to more fully participate in their own health care.

Statement	% Yes
Check for mistakes in your medical record.	69%
Check and fill prescriptions.	68%
Get results over the Internet.	58%
Conduct secure and private email communication with your doctor or doctors.	57%

Now let's imagine that a new secure online service was made available to you allowing you to locate your medical records and view them through your own secure online "personal health record" account. Now I am going to read you some things this secure online "personal health record" service would allow you to do after I read each item, please tell me, yes or no, whether or not you would use this secure online "personal health record" service for each activity.

But…

California Health Care Foundation (2005)

- **67% of Americans are concerned about the privacy**of their personal medical records--recent privacy breaches have raised their level of concern
- **1 in 8 Americans have put their health at risk**by engaging in privacy-protective behavior:
  - *Avoiding their regular doctor*
  - *Asking a doctor to alter a diagnosis*
  - *Paying privately for a test*
  - *Avoiding tests altogether*

Harris/Westin poll on EHRs and Privacy (2006)

- **42% of Americans feel that "*privacy risks outweigh expected benefits*" from health IT.**

Keeping electronic medical information private and secure remains chief among consumer concerns.

Statement	% Absolute Top Priority
The identity of anyone using the system would be carefully confirmed to prevent any unauthorized access or any cases of mistaken identity.	91%
An individual would be able to review who has had access to their personal health information.	81%
Only with an individual's permission could their medical information be shared through this network.	79%
Employers would NOT have access to the secure health information exchange networks.	68%

I am going to read you different attributes that could be part of this exchange or network and I would like you to rate the importance of each. As you respond, please keep in mind that not every attribute can be a top priority.

Americans recognize the "upside"… and the "downside"…

- Fear of misuses
  - 52% believe employer uses medical info to affect personnel or insurance benefits (CHCF Survey 2005)
  - 85% believe if genetic test results known to insurers, would refuse policies or charge more (Genetics and Public Policy Center Survey 2007)
- Three-quarters of Americans are willing to share their personal information to help public officials look for disease outbreaks and research ways to improve the quality of health care if they have safeguards to protect their identity (Markle Survey 2006).

Markle Survey
November 2006

- ***3/4 want the government to set rules* to protect** the privacy and confidentiality of electronic health information

- ***2/3 want the government to set rules****controlling the secondary uses of information*

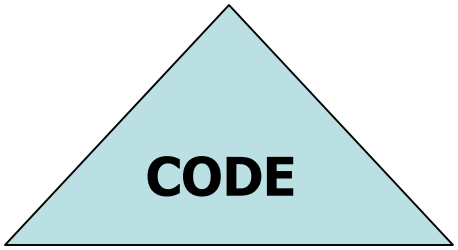
Organizational Impact

What do we know about variation in compliance?

HISPC: Sources of Variations in Business Practices

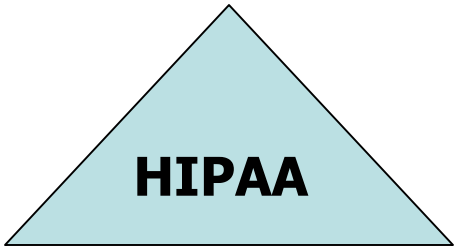
1. Variation related to misunderstandings and differing applications of HIPAA
2. Variation related to state privacy laws, scattered and often conflicting and antiquated
3. Lack of trust in applied information security
4. Cultural and business issues, concern about liability for incidental or inappropriate disclosures and general resistance to change

Variations due to uncertainty and doubt



- Federal efforts have been dominated by standards and certification
- Technical design choices have profound policy effects (Code is Law, Architecture is Policy)
- Privacy debates and policy making have been reactive instead of pro-active (guiding technical design)
- Lack of policy guidance has the potential to undermine trust

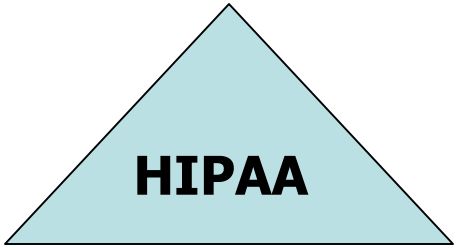
Paradigm Shift: *Technology and policy need to be developed together*



HIPAA (Health Insurance Portability and Accountability Act 1996) –

Solving 20th Century Challenges…

- Disclosure, consent
- "Covered entity" paradigm
- De-identification (18 identifiers)



Challenge

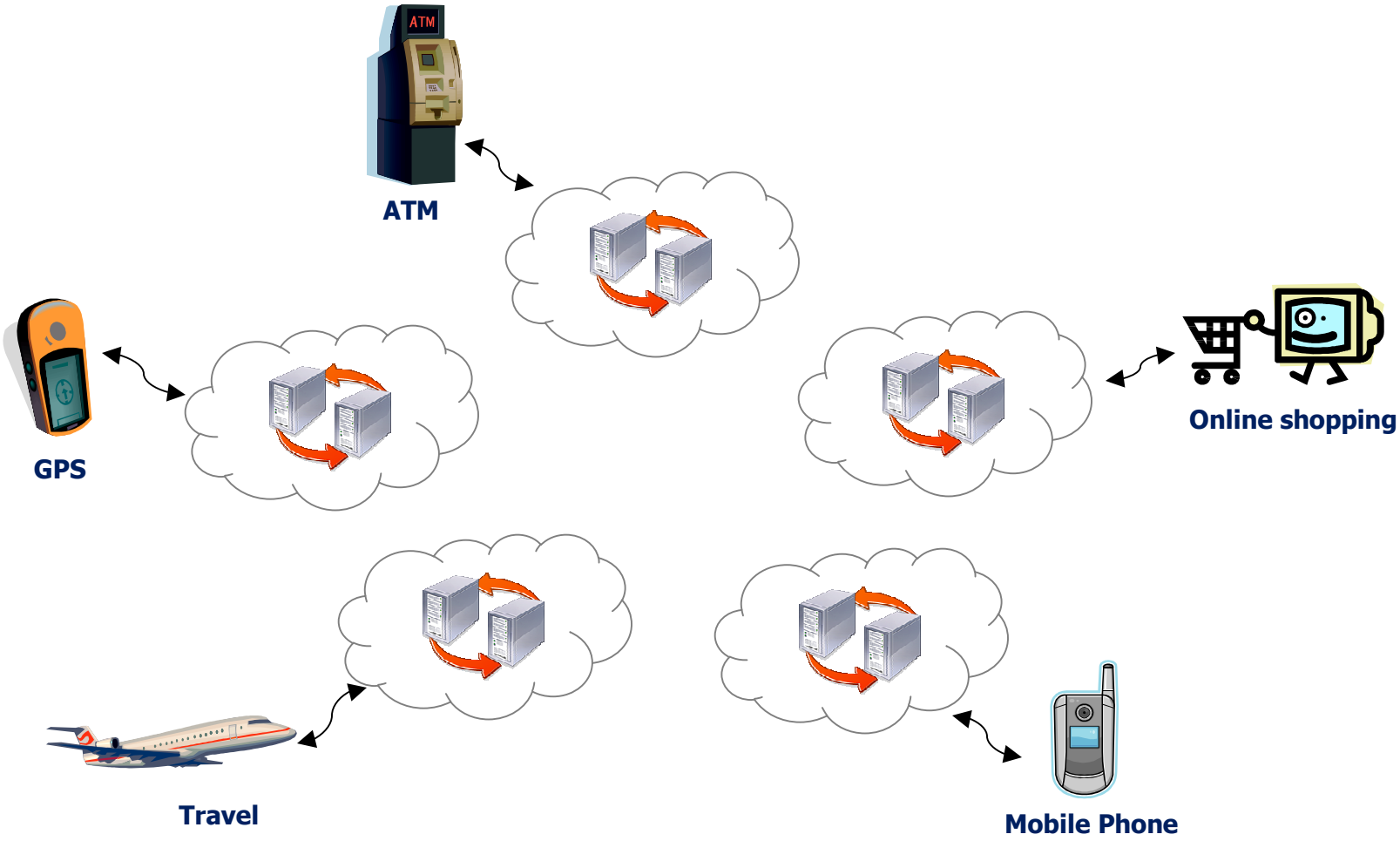
- Disclosure vs. Collection and Use of Personal Health Information
- Consent paradigms do not alone provide for protection of the consumer, rather it can burden them unfairly (consent to what? and what are the protections when consented?)
- What is "personally identifiable" is blurring, making re-identification easier
- Covered entity paradigm no longer works
- Lack of robust enforcement

Paradigm Shift: *Need a 21st Century approach*

How has the privacy landscape been changed by the Web?

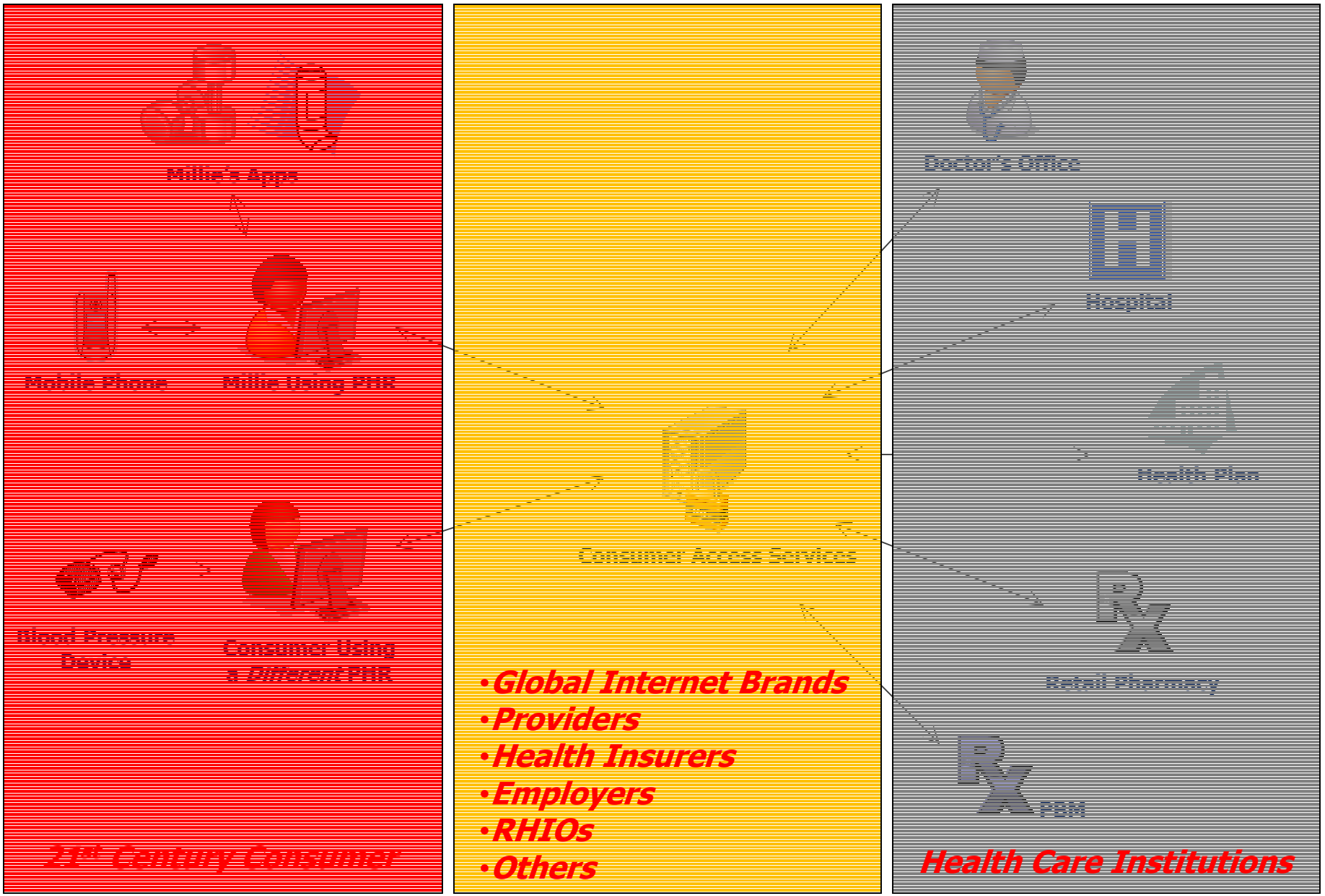
Health 2.0

Networks empower businesses and people to share information …

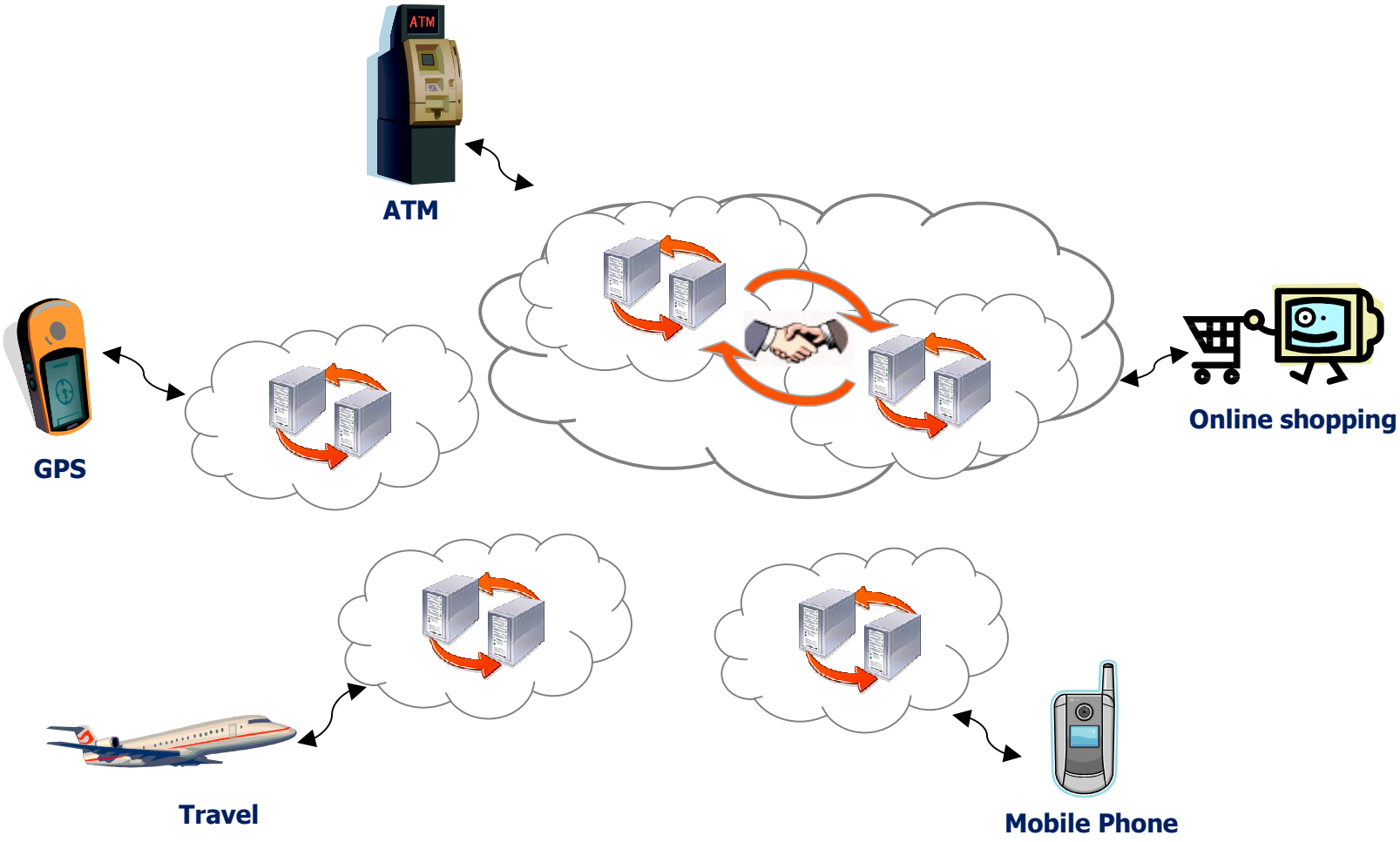


But not so much in health and health care …

- Changes in other sectors rely on a fresh openness toward consumer access to — and contribution of — information.
- Yet, health care today is not "networked."
- Consumers go through the "system" one data silo at a time.
- And much of the important information remains on paper or in the consumer's head.


Miller's Apps
Mobile Phone
Miller Using PHR
Blood Pressure Device
Consumer Using a Different PHR
21st Century Consumer
Consumer Access Services
•Global Internet Brands
•Providers
•Health Insurers
•Employers
•RHIOs
•Others
Doctor's Office
Hospital
Health Plan
Retail Pharmacy
PBM
Health Care Institutions

The power of networks depend on trust …



Changing the Current Paradigm

Focus on a 21st Century Trust paradigm that …

- Integrates policy AND technology
- Goes beyond piecemeal approaches (focus on collection, use and information handling)
- Provides a strategic frame that limits risk

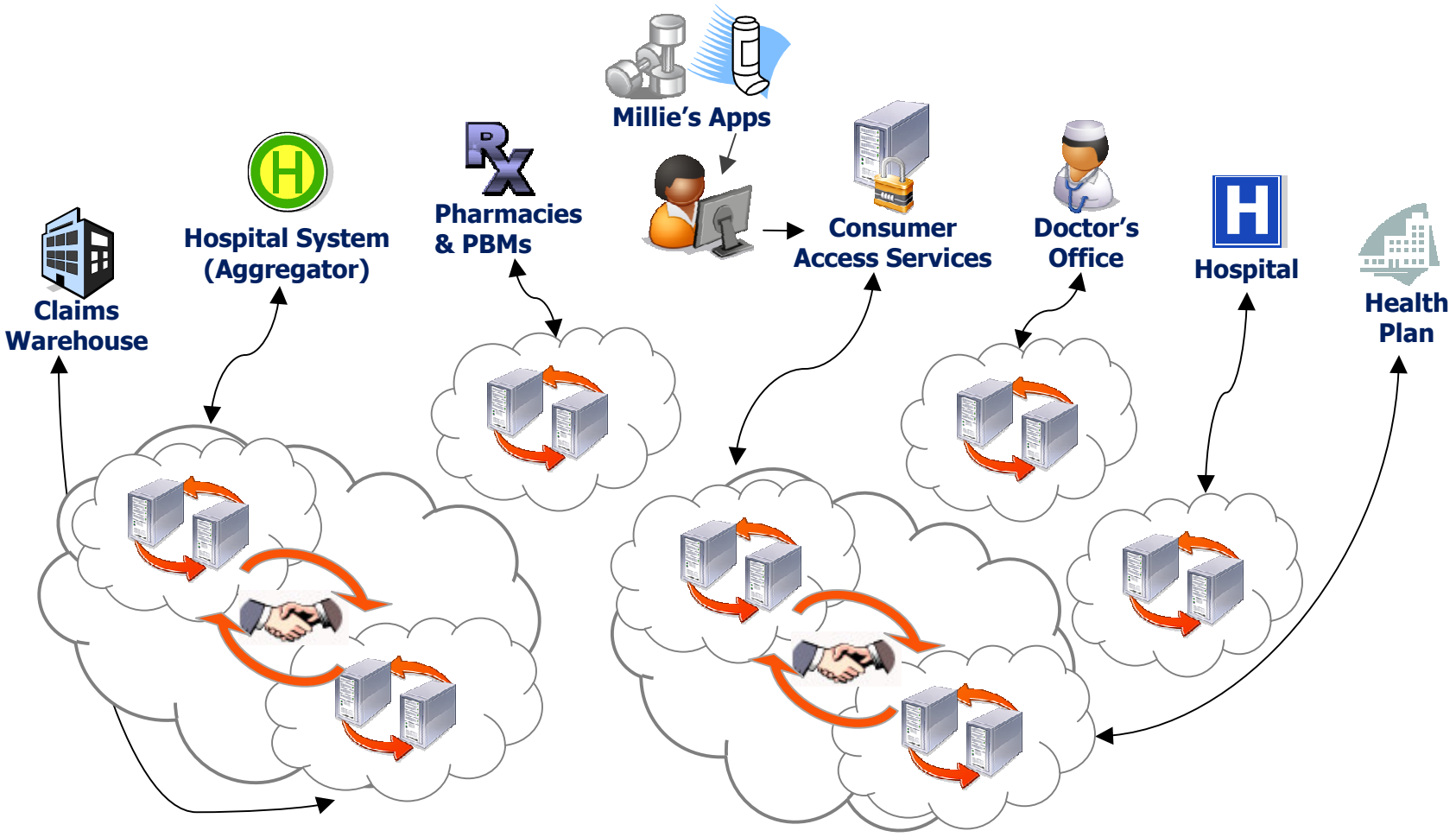
Through a common framework of attributes in which policies can be focused on preventing misuse, empowering individuals and enabling a virtuous cycle of information to shape policy and innovation

21st Century Trust Attributes

A 21st Century health information environment that fosters trust must:

1. Protect individual privacy through a set of policies that implement the core principles of fair information practice
2. Incorporate technical tools that facilitate trusted use: audit, access, authorization, authentication and accuracy
3. Promote technological choices that limit the potential for abuse (such as considering distributed architectures and separating demographic from clinical information)
4. Focus on interoperability as to allow for flexible, yet sustainable, platforms of innovation and diversity of applications

… and trust (particularly in health care) depends on …



Oversight and Accountability

Sound Network Design

Core Privacy Principles

Trust through sound information policy expectations

• Nine core privacy principles are based on Fair Information Practices in the United States, Canada, and the EU

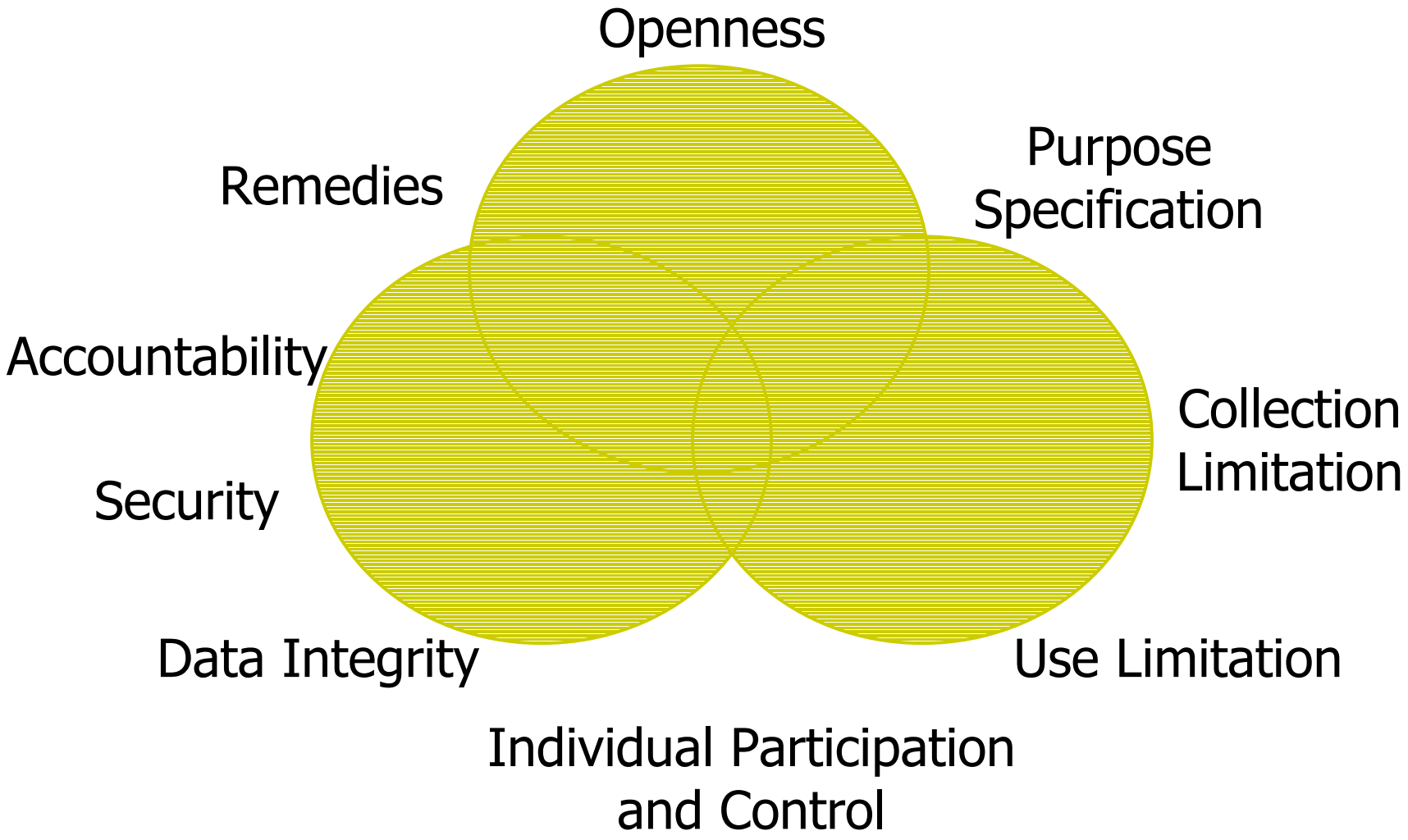
• The principles speak to:
- •Transparency
- •Specification of purpose and limitations on data collections and uses
- •Consumer access, participation and control
- •Data quality and security safeguards
- •Accountability and remedies

• The principles are fulfilled through policy **and** technology

• The principles must be **taken together** as a comprehensive approach to privacy

Core Privacy Principles

P1: The Privacy Principles are Interdependent!



Trust through extensible, practical network design

• The Internet **is** the network

•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

•Open standards should support many applications

•Information need not be centralized in order to be shared

•Data should stay where captured, and shared as needed

Sound Network Design

Core Privacy Principles

21st Century Technical Principles

1. Make it "Thin"
2. Avoid "Rip and Replace"
3. Separate Applications from the Network
4. Decentralization
5. Federation
6. Flexibility
7. Privacy and Security
8. Accuracy

Trust through governance and other enforcement mechanisms

•A policy framework is only effective if subject to mechanisms that enforce it.

• These mechanisms should empower innovations and experimentation within clear policies.

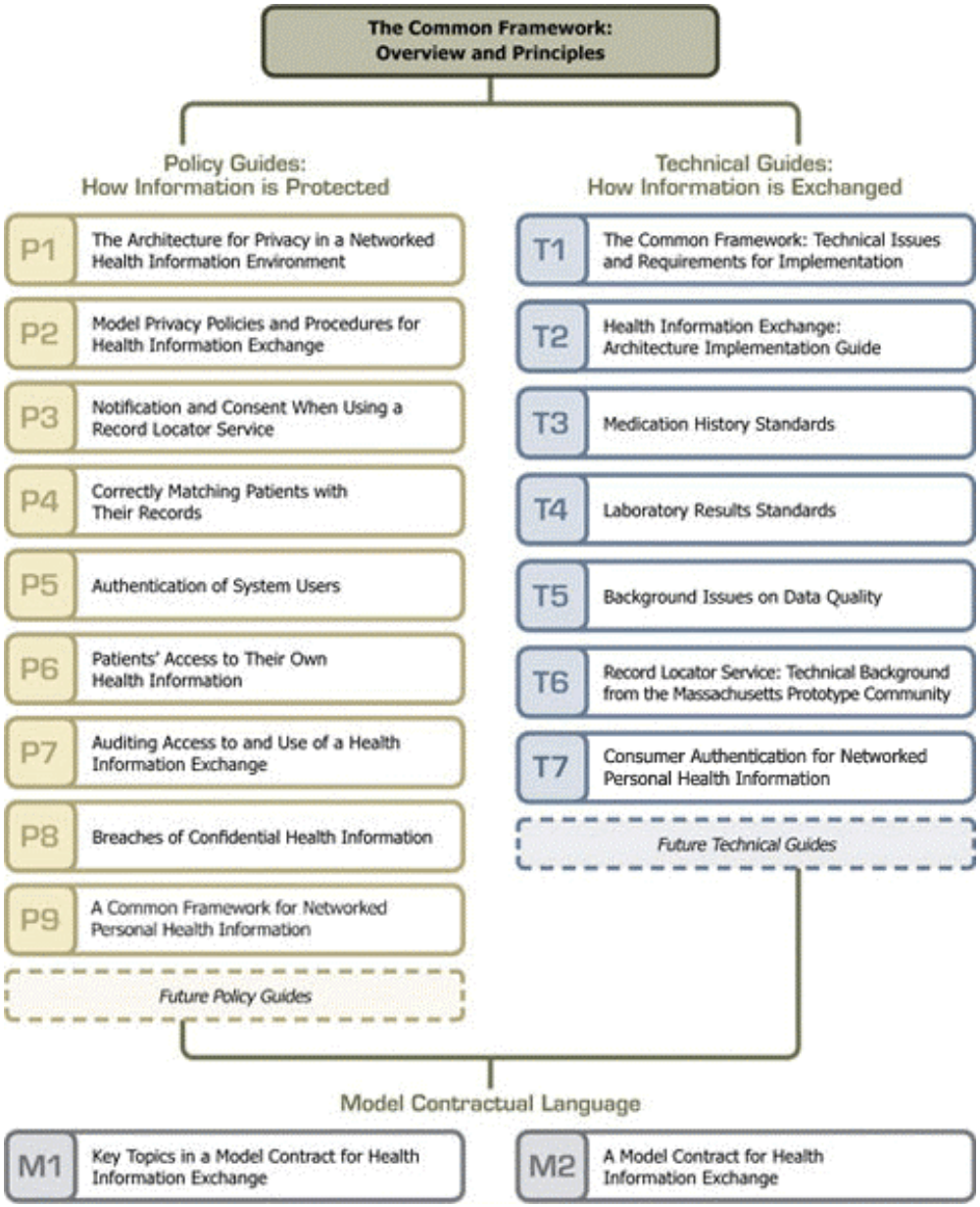
•Some uses of HIT will lend themselves to contractual enforcement within the parameters of existing state and federal laws and others will require a combination of mechanisms to establish adequate oversight and accountability.

•The governance model should anticipate future participants who may collect, transport or otherwise use patient data

Oversight and Accountability

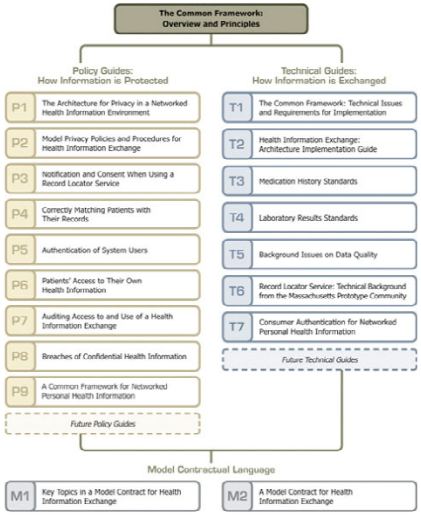
Sound Network Design

Core Privacy Principles

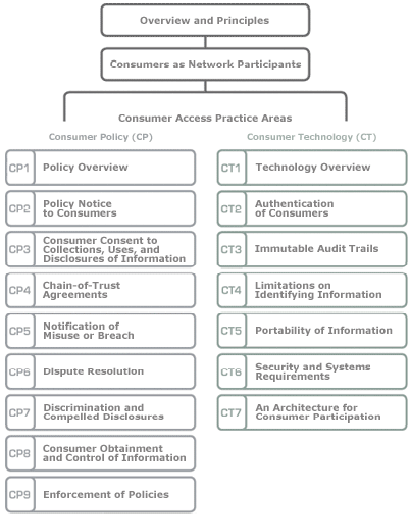

The Common Framework:
Overview and Principles
Policy Guides:
How Information is Protected
P1
The Architecture for Privacy in a Networked Health Information Environment
P2
Model Privacy Policies and Procedures for Health Information Exchange
P3
Notification and Consent When Using a Record Locator Service
P4
Correctly Matching Patients with Their Records
P5
Authentication of System Users
P6
Patients' Access to Their Own Health Information
P7
Auditing Access to and Use of a Health Information Exchange
P8
Breaches of Confidential Health Information
P9
A Common Framework for Networked Personal Health Information
Future Policy Guides
Technical Guides:
How Information is Exchanged
T1
The Common Framework: Technical Issues and Requirements for Implementation
T2
Health Information Exchange: Architecture Implementation Guide
T3
Medication History Standards
T4
Laboratory Results Standards
T5
Background Issues on Data Quality
T6
Record Locator Service: Technical Background from the Massachusetts Prototype Community
T7
Consumer Authentication for Networked Personal Health Information
Future Technical Guides
Model Contractual Language
M1
Key Topics in a Model Contract for Health Information Exchange
M2
A Model Contract for Health Information Exchange

Connecting for Health: A Public-Private Collaborative

Connecting Professionals:
Private and Secure Information Exchange



Connecting Consumers
Common Framework for Networked Personal Health Information



Oversight and Accountability

Sound Network Design

Core Privacy Principles

The First Detailed, Consensus-Based Framework for Networking Personal Health Records

Endorsed by …

AARP

Aetna

American Academy of Family Physicians

Association of Online Cancer Resources (ACOR.org)

America's Health Insurance Plans

BlueCross BlueShield Association

CapMed

Center for Democracy and Technology

Center on Medical Record Rights and Privacy

Cisco Systems Inc.

Consumers Union

Dossia

FollowMe

Google

Geisinger Health System

Health Care For All

InterComponentWare Inc.

Intuit Inc.

MedicAlert

Microsoft Corp.

National Breast Cancer Coalition

National Partnership for Women and Families

NewYork-Presbyterian Hospital

Pacific Business Group on Health

Palo Alto Medical Foundation

Partners Healthcare System

RxHub

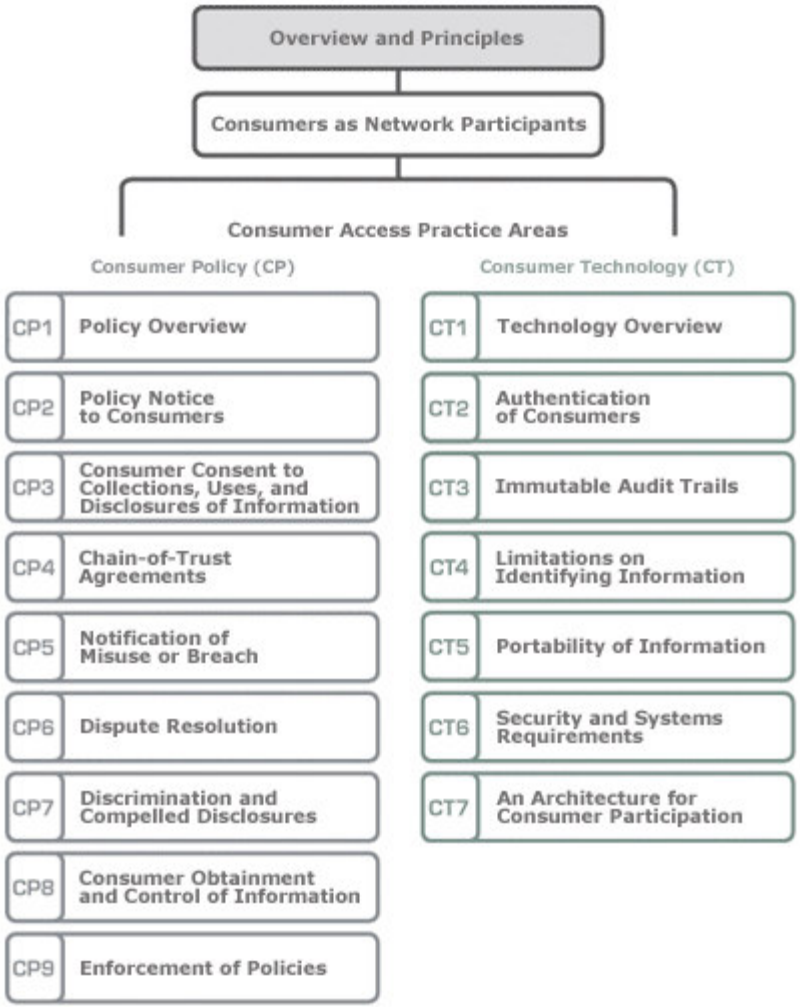
SureScripts

U.S. Department of Veterans Affairs

Vanderbilt Center for Better Health

WebMD

Common Framework for Networked Personal Health Information



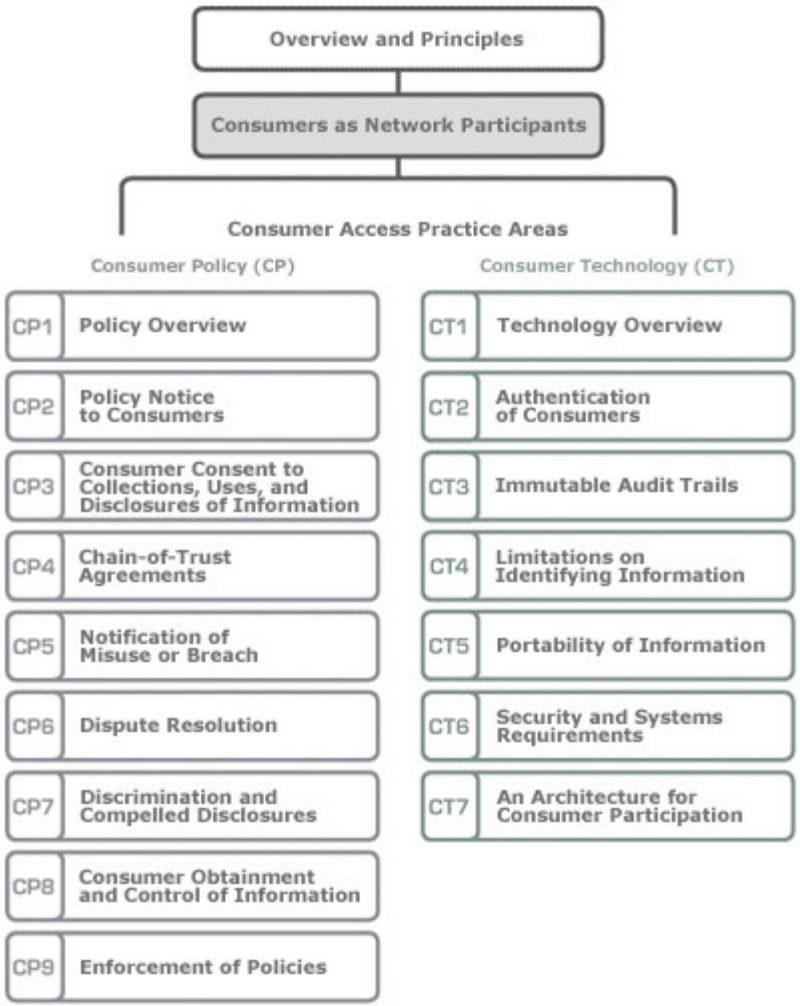
The purpose of the Connecting for Health Common Framework is embodied in "Millie."

Her character illustrates the needs of millions of U.S. adults who could benefit from greater connectivity in health and health care.

- Consumers should be able to collect, store, manage, and share copies of personal health information.

- The Common Framework is based on fair information practices and focuses on network rules, not application standards.

Common Framework for Networked Personal Health Information



Millie could manage her health the way she can manage her finances or travel.

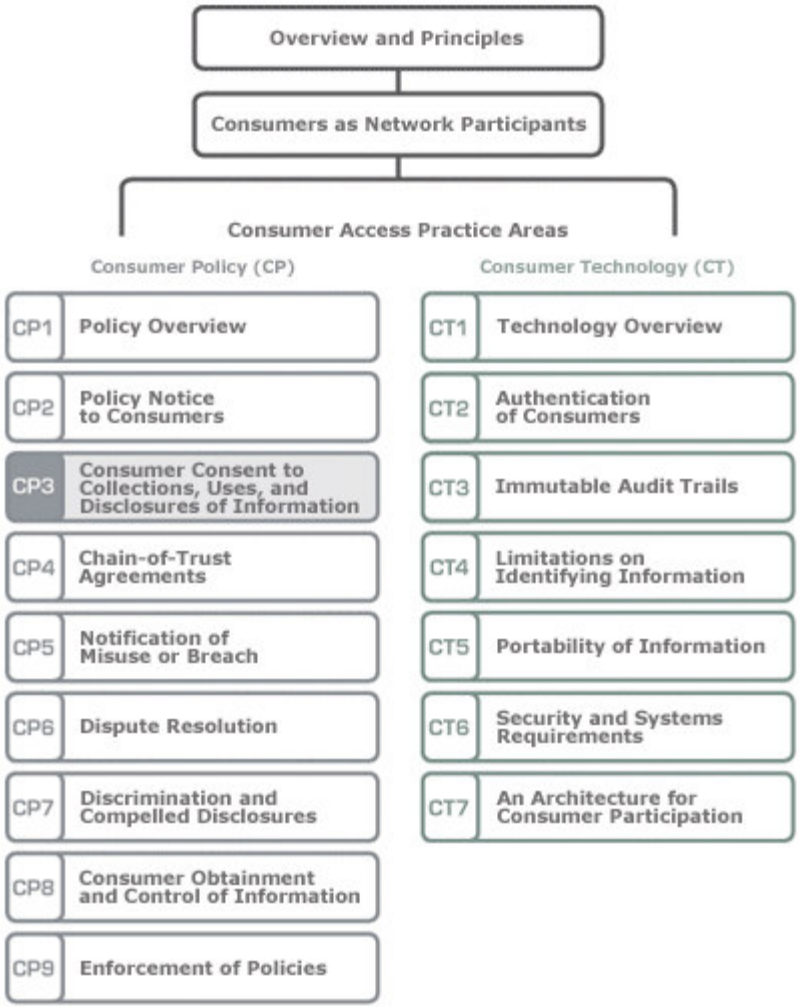
- *Download and upload critical health information*
- *Track her vital numbers*
- *Order prescription refills*
- *Get lab results*
- *Connect to professionals and communities of patients*

- *Consumers can help transform the health sector, as they have in other sectors.*

- *"Networked PHRs" are a vital tool for consumer empowerment.*

- *But to have an environment of trust, some basic rules should guide the emerging industry.*

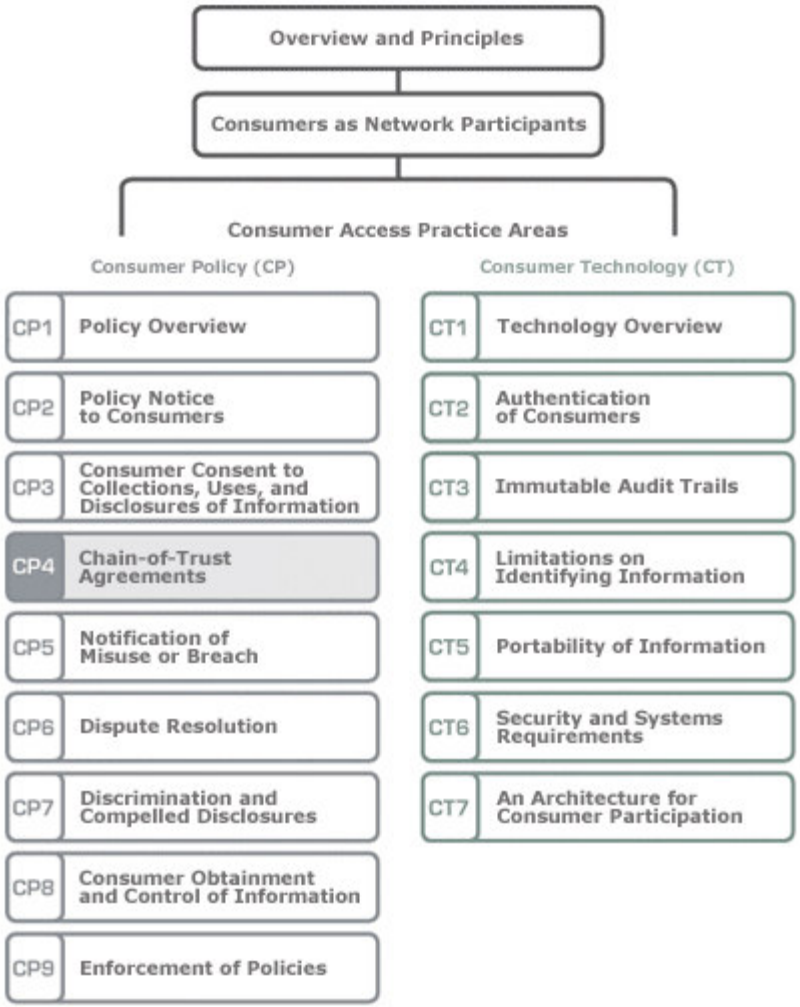
Common Framework for Networked Personal Health Information



Millie would understand and exercise meaningful choices about her information. She would be asked specifically about uses and disclosures of her personal health information.

- Obtaining the consumer's consent is a critical fair information practice.
- However, consent by itself does not adequately protect people.
- A complete framework of protections is necessary, no matter the 'I agree' statement.
- Specific, "independent consent" is advisable for practices that would be unexpected by a reasonable consumer.

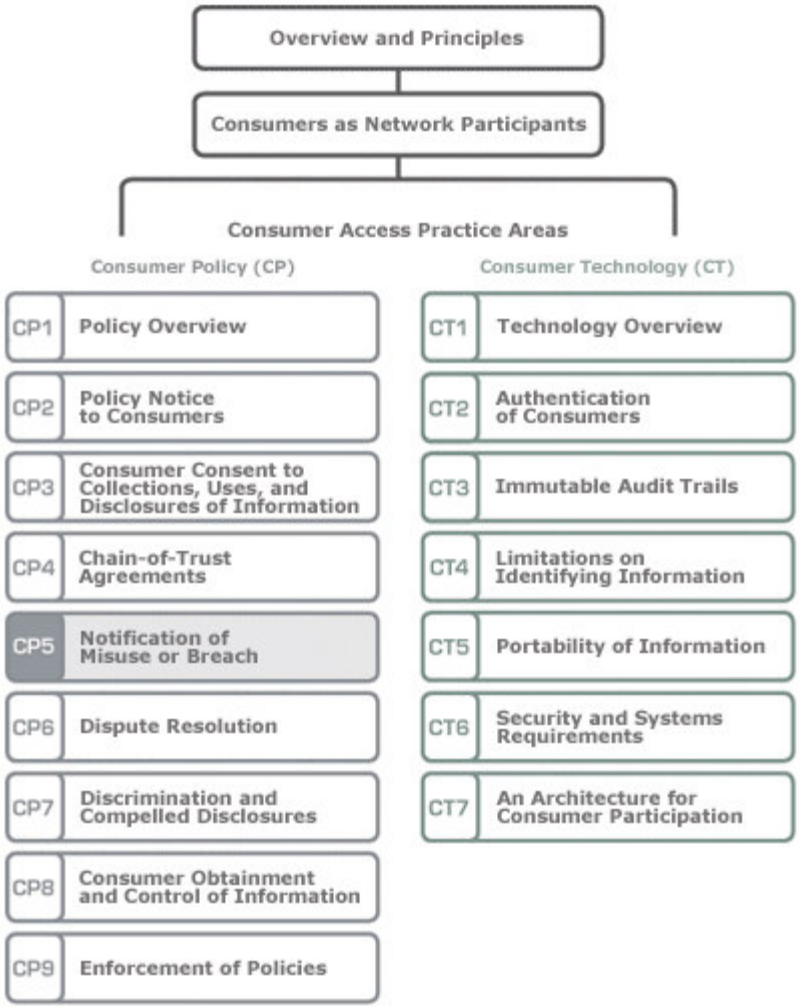
Common Framework for Networked Personal Health Information



The organizations that touch Millie's health information would be Contractually bound to handle the information according to specified policies. For example, the policies would disallow business partners from assembling unauthorized profiles about Millie.

- Contracts are one mechanism to bind parties to policies.
- Chain-of-trust agreements should disallow unauthorized uses of information.
- There are limitations to chain-of-trust agreements, including inconsistent enforcement and scaling difficulties.

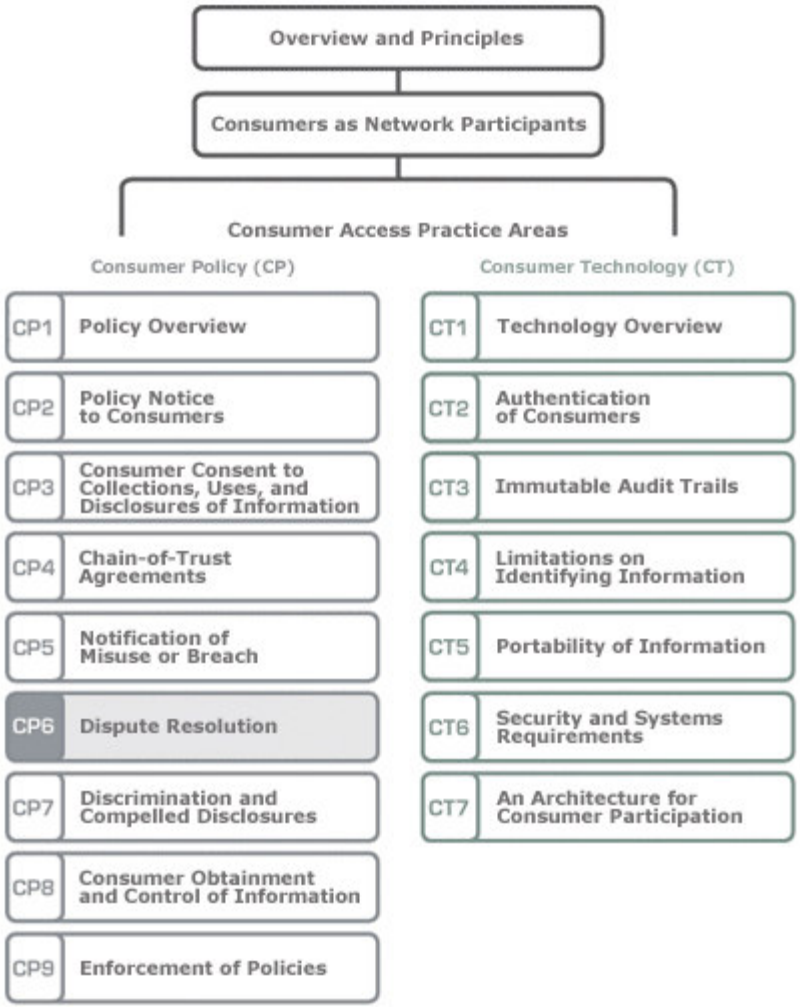
Common Framework for Networked Personal Health Information



If Millie's information or identity becomes compromised because of a mistake, data leak, or fraud, Millie would be notified about it in a timely way. She would be told what she can do, and what others will do, to limit any harm.

• There should be policies to notify affected consumers in the event of a potentially harmful breach of information.

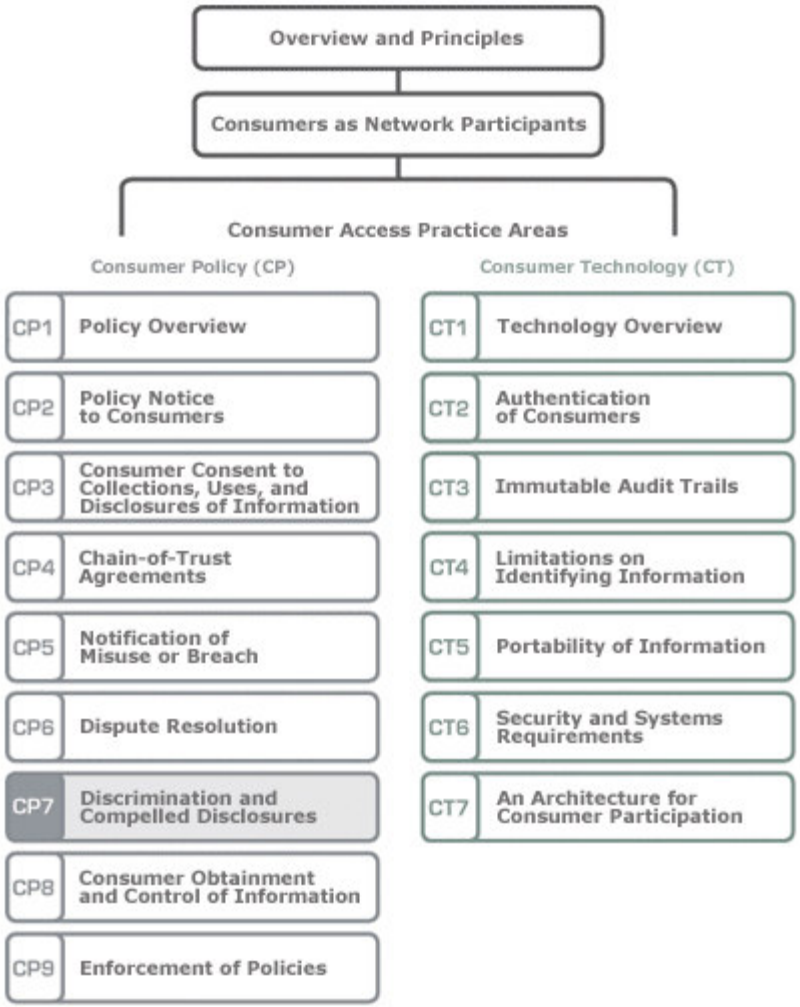
Common Framework for Networked Personal Health Information



If Millie has a problem with a service, or finds an error about her information, she would be able to easily figure out the process for resolving it.

• There should be mechanisms to resolve disputes such as breach or misuse, data quality or matching errors, allegations of unfair or deceptive trade practices, etc.

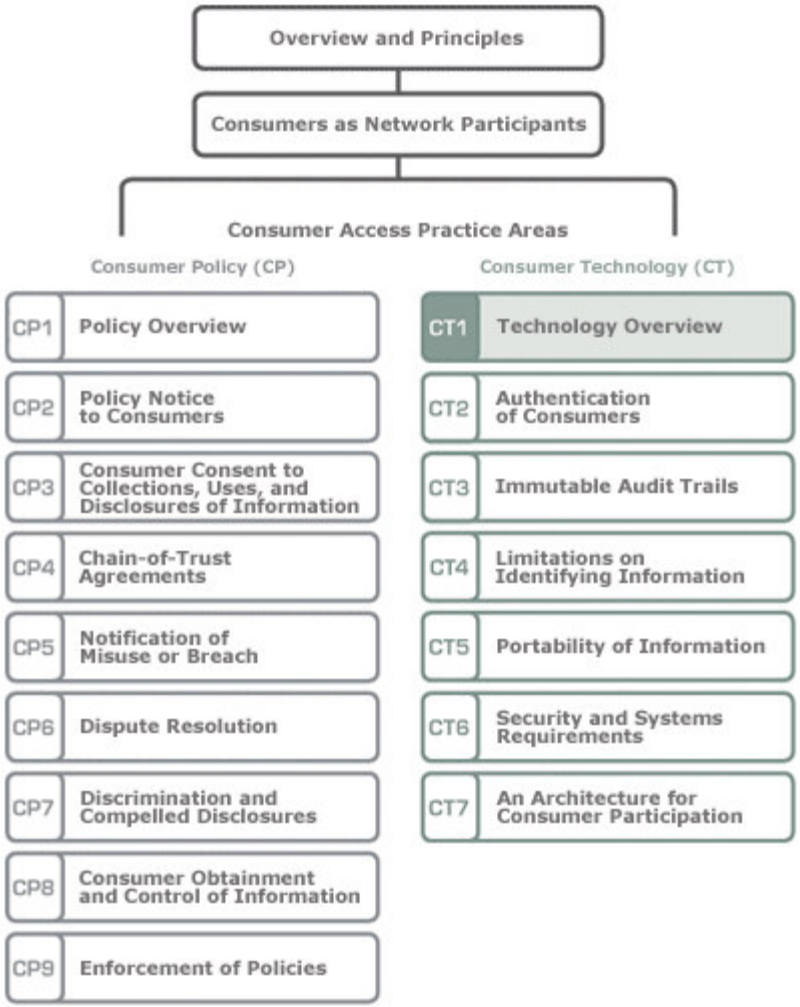
Common Framework for Networked Personal Health Information



Millie wouldn't lose her job, insurance, or other benefits because of information about her on the network. She also wouldn't be forced to allow insurers or employers to see her information in order to get a job or benefits.

- Some new services will co-mingle information from professionals and consumers.
- It is important to disallow discrimination based on information in PHRs or similar consumer tools.
- Participating organizations should take a strong stand against "compelled disclosures" (i.e., when consumers must allow organizations access to personal information in their PHR as a condition of employment, benefits, or other critical services.)

Common Framework for Networked Personal Health Information

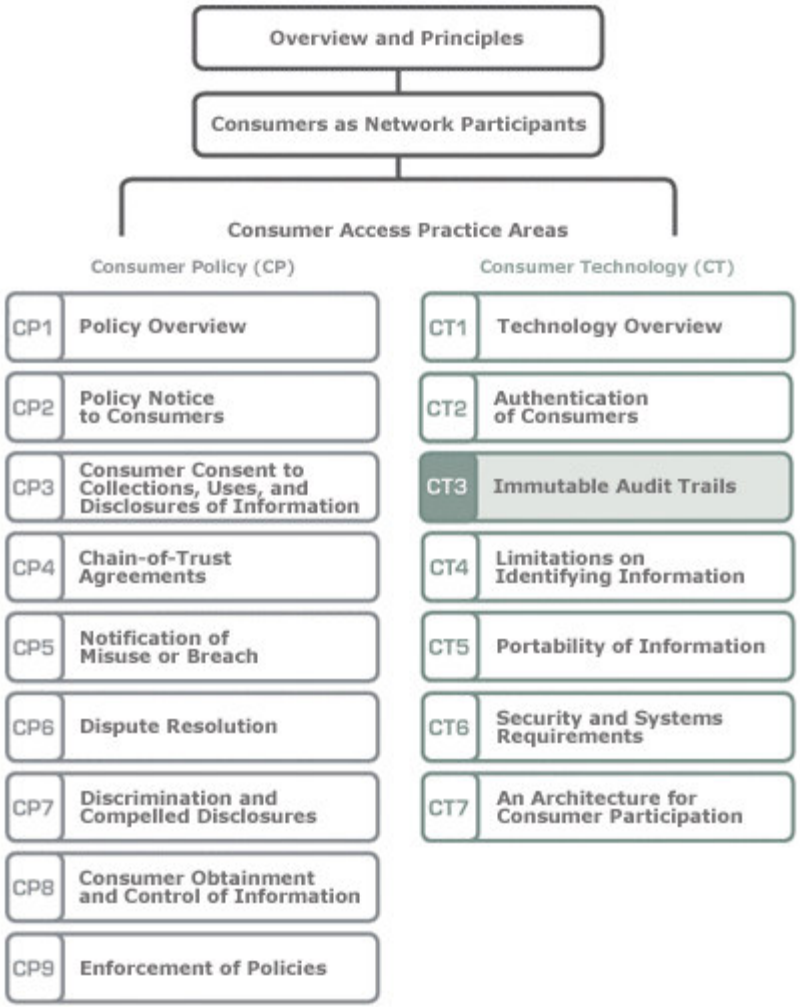


Millie's health information moves many places, in lots of different bits and bytes.

Each organization touching information about her has different roles and plays by somewhat different rules.

- Health data streams are enormously complex, resulting in copies of information being held at many different points.
- Information can be combined to build revealing profiles of individuals.
- As consumers become network participants, new "consumer data streams" are being created.
- Consumers need better tools and assurances that their information will be handled according to fair information practices.

Common Framework for Networked Personal Health Information



Millie would be able to see who has accessed her accounts and the information in them. It would all be tracked, and accessible to her anytime.

•PHRs and supporting services should maintain an easy-to-comprehend, user-accessible, and clearly labeled electronic audit trail containing immutable entries that pertain to the consumer's account, data, and policy consent.

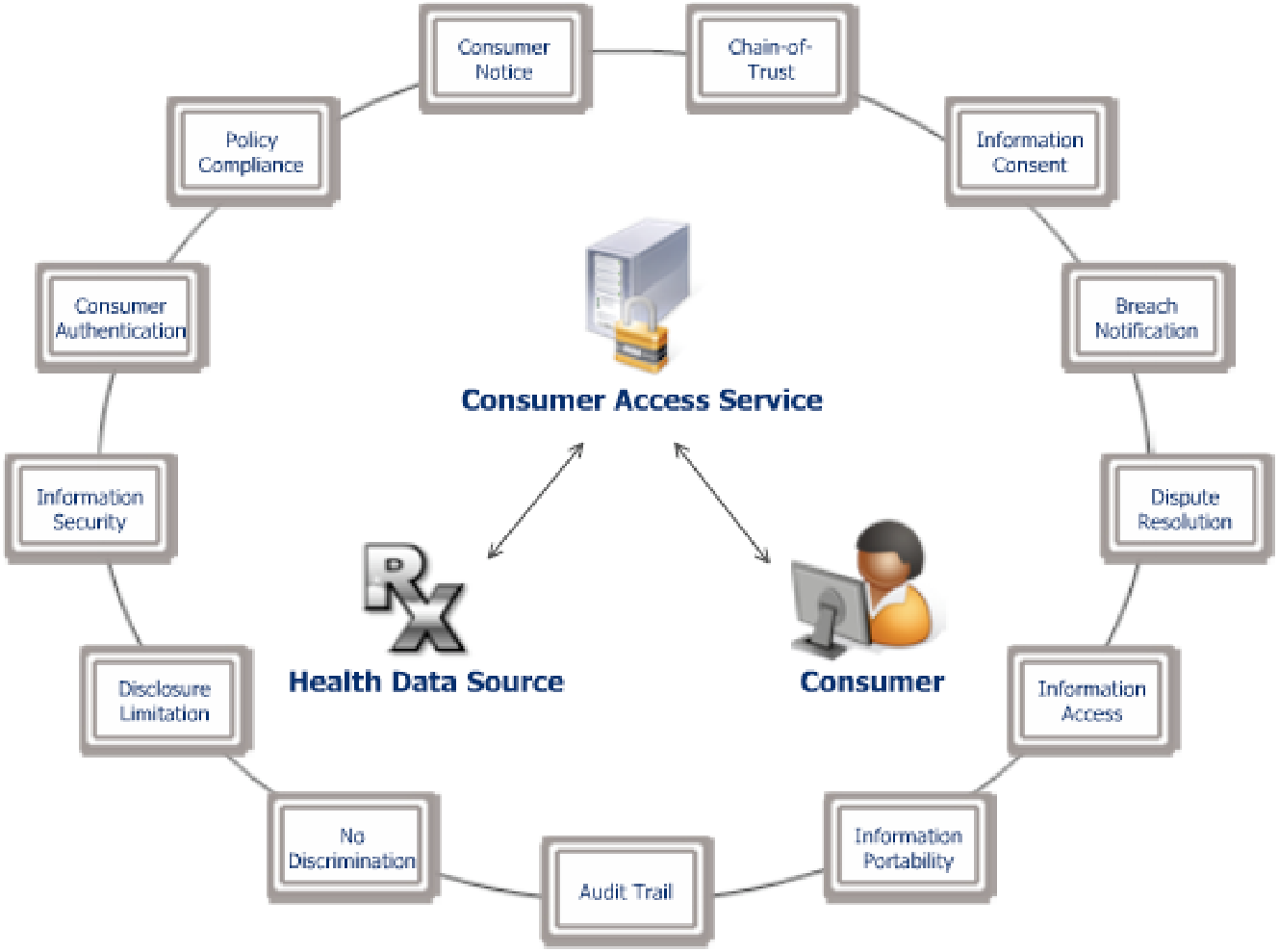
Connecting for Health Principle	Common Framework Resource
1. Openness and transparency:	**CP2**: Policy Notice to Consumers
2. Purpose specification:	**CP2:** Policy Notice to Consumers **CP3:** Consumer Consent to Collections, Uses, and Disclosures of Information **CT4:** Limitations on Identifying Information
3. Collection limitation and data minimization:	**CP2:** Policy Notice to Consumers **CP3:** Consumer Consent to Collections, Uses, and Disclosures of Information **CT4:** Limitations on Identifying Information

Connecting for Health Principle	Common Framework Resource
4. Use limitation:	**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:	**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 TrailsCT5: Portability of Information

Connecting for Health Principle	Common Framework Resource
6. Data quality and integrity:	**CP6:**Dispute Resolution **CP8:** Consumer Obtainment and Control of Information **CT2:** Authentication of Consumers **CT3:** Immutable Audit Trails
7. Security safeguards and controls:	**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

Connecting for Health Principle	Common Framework Resource
8. Accountability and oversight:	**CP4:** Chain-of-Trust Agreements **CP5:**Notification of Misuse or Breach **CP6:** Dispute Resolution **CP9:** Enforcement of Policies **CT3:** Immutable Audit Trails
9. Remedies:	**CP5:**Notification of Misuse or Breach **CP6:** Dispute Resolution **CP9:** Enforcement of Policies

When taken together, the practices enhance participation and protect personal health information



What Markle Set Out to Explore

- *Many surveys since 2005 have explored Electronic Health Records (EHR) systems and privacy issues involved*
- *But major services now unfolding for individuals to create, store, and process their health information online, apart from EHR organizational systems*
- *These PHRs being offered by major health insurers (e.g. Aetna), employers (Dossia), HMOs, and Internet companies (Microsoft, Google, Revolution Health, WebMD, Intuit, etc.)*
- *Some under HIPAA (if by covered entity), but others not*

Survey Methodology

- *Questionnaire developed by Josh Lemieux and Alan Westin, with Markle staff input*
- *Sample creation, fieldwork and data production by Knowledge Networks*
- *1,580 respondents, representative of total adult (18+) population, both on and not on the Net*
- *Responses collected by special online process, May 13-22, 2008*
- *Knowledge Networks places error rate at +/- 2.5%*
- *Estimates of millions represented by results based on Current Population Survey estimate of adult US population at 228M*

Markle Survey: Key Findings

- Four in 5 believe that online PHRs would be beneficial in managing their health and health care.
- Nearly half the public expresses some interest in using one.
- Among those not interested, concern for privacy is the most frequently cited reason why.
- Majorities of 87 percent to 92 percent say six key privacy practices are factors in their decision to use an online PHR.
- More than 90 percent said their express agreement should be required for each use of their online health information.
- More than 75 percent said each of four possible policy enforcement mechanisms would be effective.

For more information:

www.connectingforhealth.org