Common Framework for Networked Personal Health Information: Consumer Technical (CT) Briefs, June 2008

How "Millie" — a 21st Century consumer — would benefit under a Common Framework to help her obtain and control electronic copies of her personal health information and connect to health information services.

Overview and Principles

*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.*

CT1 Technology Overview

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.

CT2 Authentication of Consumers

Millie would be able to prove she is who she says she is, and link to her information in various systems, without an enormous burden to herself. However, the methods would make it extremely hard for someone to pose as her.

CT3 Immutable Audit Trails

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.

CT4 Limitations on Identifying Information

Unauthorized organizations would not be allowed to build profiles about Millie by combining her information with other databases. The organizations that touch her data would take care not to disclose identifying information about her, unless there's a clear need for it agreed to by Millie.

Consumers as Network Participants

Millie could manage her health the way she can manage her finances or travel. For example, she could choose applications to download and upload critical health information, track her vital numbers, order prescription refills, get lab results, and connect to professionals and communities of patients — all in an electronically interconnected environment that she trusts.

CT5 Portability of Information

Millie would be able to download copies of information about her for personal use. In the future, she would be able to push a few buttons to move her health information electronically from one service or application to another, if she wants to.

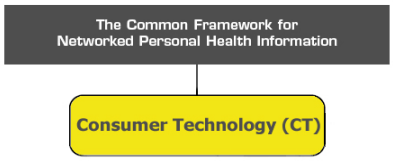
CT6 Security and Systems Requirements

Millie would know that the best practices for securing her information are in place, and they will continue to be updated as appropriate.

CT7 An Architecture for Consumer Participation

The way the network is set up, Millie's information wouldn't need to be in big repositories just so it could be shared. If she wanted to put it in a repository, she would be able to, but there would be an easy way to find her information when she asks for it, without relying on one big database.

See Consumer Policy (CP) Briefs



Common Framework for Networked Personal Health Information: Consumer Technology (CT) Briefs, June 2008

Key messages of the technology resources in the Common Framework:

Overview and Principles

- 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.

CT1 Technology Overview

- 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.

CT2 Authentication of Consumers

- Sound authentication practices are a cornerstone of information security.
- There is no magic bullet, or one-size-fits-all approach, to authentication.
- Depending on their capabilities and relationship with consumers, PHRs and supporting services should consider using in-person proofing, 'bootstrapping' of in-person proofing by other organizations, and remote proofing as alternatives to in-person proofing.

CT3 Immutable Audit Trails

- 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.

Consumers as Network Participants

- With new Internet-based tools, consumers can help transform the health sector, as they have in other sectors.
- "Networked personal health records" (PHRs) are a vital tool for consumer empowerment.
- Some basic rules should guide the emerging industry.

CT4 Limitations on Identifying Information

- PHRs and supporting services should limit the scope of the identifying data disclosed to third parties to only those that are reasonably necessary to perform the specified and consumer-authorized function(s).
- Care should be taken to limit the release or exposure of electronic identifiers that can be directly or indirectly tied to an individual, including IP address, cookies, and web beacons.

CT5 Portability of Information

- Consumers should be given the ability to compile their health data electronically from multiple sources for personal use.
- Consumers should be able to download their data into applications they control.
- The ideal future state is one in which the consumer can transfer personal data electronically between PHRs and supporting services.

CT6 Security and Systems Requirements

- PHRs and supporting services should adopt best industry practices for data transaction and storage security to enforce privacy policies and practices and, in doing so, build network and consumer trust.

CT7 An Architecture for Consumer Participation

- **Connecting for Health** technical principles should shape how PHRs and supporting services fit within a sound and flexible architectural approach to a Nationwide Health Information Network (NHIN).

— *See Consumer Policy (CP) Briefs*