

Opinion: Benefits of personal health records will eclipse privacy concerns

Jay Cline

May 7, 2008 ([Computerworld](#))

In five years, the privacy debate over personal health records will be over, and you and I will be storing our medical records at a central location.

Why? Because the benefits of better care and less paperwork will outweigh our current fears about breaches and inappropriate data-sharing. Whether that central location is Redmond, Mountain View or Boston will depend on whom we trust most with our medical information.

What is an electronic personal health record (PHR), anyway? I recently reviewed the specifications of five key players' platforms, and I'd say the prevailing model will have these six core features:

1. A single repository that integrates files of varying formats from multiple sources.
2. Files that are related in a way that provides cohesive, longitudinal records over time that are easily searchable.
3. The trust of doctors, who will believe the files are accurate and authentic.
4. Records that are understandable to the patient.
5. The ability for patients to add information and flag errors.
6. Patient control over who sees what.

I don't see these records being stored on cards we carry around, because I don't think cards can provide all of these features. These "records" are going to be Web-accessible databases stored on a server somewhere.

What kinds of records will they contain? The sky is really the limit on this question. Promised data sets include the following:

- Prescriptions, food and drug allergies, and immunizations.
- Past illnesses and hospitalizations.
- Results from tests, physical exams and clinical trials.
- Information from implanted medical devices.

- Health insurance information and claims.
- Living wills and organ-donor instructions.
- Exercise and diet records.
- Genomic information.

With this kind of sensitive information concentrated in one place, privacy and security will become mission-critical. Repeated breaches could irreparably undermine confidence in and adoption of the system.

So, what if you took the most hardened privacy advocates, put them in a room, and told them they had to issue the ideal privacy and security requirements for these PHR platforms? What would they say?

Judging from past statements, I think their concerns would mirror the seven [EU-U.S. Safe Harbor](#) principles:

1. **Notice.** Users would need total awareness of what records were being added to their PHRs.
2. **Access.** Users would need full access to any record in their PHRs, and those records would need to be easily understandable.
3. **Data integrity.** Users would need to be able to flag and amend any inaccuracies and supplement records with their own input.
4. **Security.** Not just “reasonable” security, but the best available security would need to be deployed, including encryption of data at rest. All instances of a patient's record being accessed would need to be logged.
5. **Choice.** Participation would need to be voluntary, and users would need to be able to have granular, field-level control over who gets to see what parts of their records, and for what purpose.
6. **Onward transfer.** Users would need to be able to restrict how their file is shared and have some recognizable way to know that data recipients had been security-certified.
7. **Enforcement.** Users would need to see reliable evidence that the privacy and security of the platform had been regularly and independently verified. And they must have an independent way to resolve their privacy concerns.

But the advocates would also say that any PHR platform provider is, by itself, unable to ensure that data is safe and private once it leaves the

platform. [Microsoft](#) or [Google](#), for example, can't prevent a diabetes Web site from mishandling data it extracts from the platform.

Or could they? If a few companies emerged as the PHR platform providers of choice, couldn't they form a coalition similar to the Payment Card Industry Data Security Council? Couldn't they similarly fine or expel errant platform participants? Visa has been far more effective at enforcing its PCI standards, after all, than the Department of Health and Human Services has been at enforcing HIPAA.

While there's no traction yet on a PCI-type standard for PHRs, the question of which laws cover and should cover PHRs is the focus of debate right now. The leading PHR platforms I reviewed are not tied to a medical entity like a hospital or health insurer, and therefore are not covered by HIPAA.

That said, free-standing PHRs are subject to consumer-protection laws that prohibit false statements and impose security requirements.

“In this environment,” explained Ann Waldo, chief privacy counsel at [Dossia](#), one of the PHR platform providers, “the details of a PHR's privacy statement are crucial. They need to contain the full range of protections appropriate to the private and sensitive health information the PHRs will be safeguarding.”

Once those promises are made, they become enforceable by the [Federal Trade Commission](#), state attorneys general and plaintiffs' lawyers.

So I think the argument for HIPAA to save the day is a canard. I think the privacy questions will resolve themselves because companies' profits and reputations depend on it. Enormous first-mover advantages will accrue to the company that can meet and exceed the privacy expectations of the most cautious prospective users.

Who will emerge on top? Here are the leading candidates:

- **Microsoft.** Last October, it launched the HealthVault, a platform where 40 partners have brought their interoperable applications and devices. Users don't pay to start an account on the platform.

Microsoft has the advantage of being the provider of software nearly everyone is comfortable using.

- **Google.** The company that aims to organize the world's information has launched a limited pilot at a Cleveland hospital to test its own version of a PHR platform -- also free to the user. Google has the advantage of having an unparalleled reputation of being able to provide exactly what kind of information we want when we want it.
- **Dossia.** Eight corporations — including AT&T, [Wal-Mart](#) and Intel — have joined forces to create their own platform tied to Children's Hospital in Boston. The platform will be free for their employees' use this year or next and will ultimately run as a nonprofit open to all. Dossia's advantage is twofold: a ready supply of insurer-provided information and the trust people still place in their employers.
- **WebMD.** The New York-based health information portal runs a fee-for-service Health Manager where users can store and disseminate their personal health records. WebMD's advantage may be its simplicity. It may also appeal to many Fortune 500 employees, because it is already populated with their health care data.
- **Revolution Health.** Run by former AOL CEO Steve Case, the Washington-based competitor of WebMD offers the fee-for-service Health Records Express, a place to store and disseminate medical records.

I don't think it's a matter of if you and I will join one of these platforms, but when. And the one we join will depend not just on privacy, but more broadly on whom we trust. On this question, it's still anyone's game.

Jay Cline is a former chief privacy officer at a Fortune 500 company and is now president of [Minnesota Privacy Consultants](#). You can reach him at cwprivacy@computerworld.com.