Dissenting Statement on
PHR Certification Process

March 13, 2007

The Honorable Michael O. Leavitt
Chairman
American Health Information Community
200 Independence Avenue, S.W.
Washington, D.C. 20201

Dear Mr. Chairman and the American Health Information Community:

We, the undersigned members of the AHIC Consumer Empowerment Workgroup, dissent from the Workgroup Recommendation 1 that HHS encourage a certification process for electronic personal health records (PHRs.)

We acknowledge a need for federal governmental leadership that accelerates the potential of PHRs to empower the consumer. However, certification should not be a governmental focus at this time. The risks outweigh any potential benefits. If this recommendation goes forward, it will create momentum for certification that is likely to ignore a broad range of critical policies and, as well, stifle innovation by prematurely locking in current approaches to PHRs and deterring new entrants in a field that is newly developing. For the reasons outlined below, a premature process for certification — even if it begins as voluntary and attempts to limit itself to privacy, security and interoperability — risks undermining opportunities to empower consumers and improve the quality of care.

The PHR landscape is immature in several ways. First, we cannot yet define which features or requirements will prove to be most valuable to American patients and families. Innovative models for a wide range of services for consumers have not been explored. Second, the policies that might potentially be fulfilled by certification have not been developed. Third, the technology and data standards — including those recommended by HITSP to support the AHIC use cases — also remain largely untested in real-world settings. Each of these gaps is acknowledged in the Consumer Empowerment Workgroup's findings and recommendation.

Certification will not drive a marketplace for PHRs, and thinking about the issue as one of creating a marketplace is misguided. Rather, a more appropriate focus would be to collaborate broadly to develop policies that establish consumer confidence in the accuracy, confidentiality and limitations on secondary use of their records, and on how to make PHRs useful to consumers. If these two things can be achieved, they are far more likely than certification to drive consumer adoption.

We believe the primary focus today should be on developing recommended privacy and security policies for the use in PHR services with trusted exchange of personal health data. This is consistent with Recommendation 2.1 made by the Consumer

Empowerment Workgroup at the AHIC meeting on Jan. 23, 2007. Once we have identified a set of policies and practices for PHRs, it will be appropriate to determine what kind of enforcement process is best suited to each type of policy. We should consider a full range of enforcement mechanisms to achieve robust privacy protection and interoperability. This spectrum includes regulatory enforcement, contractual agreements, procurement, self-certification with validation, third-party certification, and statute.

We recognize that the Consumer Empowerment Workgroup is not explicitly recommending certification of product features and functions at this time. However, we submit that for HHS to encourage a process for certification of standards and interoperability implies a certain level of functionality. We also note that the workgroup does not recommend that the government require its vendors to use certified PHRs or that it make certification a prerequisite for federal funding. This demonstrates our point that it is too early to adopt this recommendation.

We have the following specific concerns about any focus on PHR certification at this time:

- **PHRs are different from EHRs:** Proponents of PHR certification point to the launch of CCHIT's certification of EHRs. We believe the two domains are dramatically different — and not only because EHRs are more mature by nearly a decade. High initial capital outlays and significant financial exposure are barriers to physician adoption of EHR products, and market stabilization is therefore considered vital. By contrast, access to PHR applications is free or of minimal cost, switching costs are low, and therefore the proposed advantages of certification of EHRs do not apply to PHRs.

  In addition, we note that at most only 24 percent of U.S. physicians are using some form of EHR products.[1] Indeed, the adoption rate is closer to 9 percent for EHR systems most likely to have data of high value to consumers.[2] It is likely that PHRs will develop with many approaches to data acquisition and sharing, including self-population, use of claims data, direct access to pharmacy, laboratory, and monitoring data, scanned documents, and community-derived content. We see no reason to pick any one class of data as deserving special and limiting attention at this time.

- **Software certification does not necessarily assure privacy or security protections:** Proponents of PHR certification cite a need to provide assurance

---

[1] Blumenthal D, DesRoches C, Donelan K, Ferris T, Jha A, Kaushal R, Rao Sowmya, Rosenbaum S. Health Information Technology in the United States: The Information Base for Progress. Available at: http://hitadoption.org/downloads/annual_report_2006.pdf

[2] National Center for Health Statistics. National Ambulatory Medical Care Survey. Available at: http://www.cdc.gov/nchs/products/pubs/pubd/hestats/electronic/electronic.htm

to consumers about privacy in order to increase adoption of (presumably) certified PHR products. However, we submit that privacy practices are not primarily software product attributes. Instead, they depend on behavioral conformance to a broad set of policies that bear upon the data source, the sponsor of the PHR, the hosting service of the PHR, and its users. We are not aware of circumstances where "privacy" has been certified for a software product. Indeed, certification of PHR applications alone will be inadequate because true privacy and security protection must exist throughout an entire chain of handoffs between data sources and the end-user application. Further, we have seen no published research suggesting that certification will adequately address public concerns about privacy or encourage greater adoption and use of PHRs. Moreover, certification provides no redress for breaches of personal health information or inappropriate secondary uses. It can create false assurances for the public. We therefore believe that the potential harm of a voluntary privacy and security certification at this time outweighs any potential benefits.

- **Early "winners" can deprive consumers:** We do not yet know which approaches to PHRs will prove valuable to consumers. Any certification at this time effectively declares "early winners" and prescribes a required path for market success. This will be true regardless of whether certification begins as "voluntary." If federal agencies were required, for example, only to procure certified PHR products, it is likely that many innovative approaches to empowering patients and families would be unavailable to federally sponsored populations. Certification "locks in" a definition of systems around today's dominant product offerings, which are based on our experience of yesterday. Relying on yesterday's technology experience almost invariably leads to systems that fail to meet tomorrow's needs. Over time, certification can reward mediocrity, encourage an industry of legacy systems, and increase the costs of switching to new and better approaches.

- **Certification can freeze out innovators:** The administrative and financial burdens of conforming to a certification process fall hardest on smaller players (from which new innovations often spring). These burdens are not simply the cost of a certification review, but the very substantial operating costs of conforming to the third-party review process.

- **Given their inherent inflexibility, certification criteria are difficult to get right.** If the bar is set too low, then too wide a range of applications will be certified. The result will be meaningless to consumers or, worse, give them false expectations about protections to their data. If the bar is set too high, then new innovators will be blocked and the consumer will be deprived of improved services. This problem of setting optimal criteria exists in any market, but it is particularly resonant in an immature one. If, at some future time, PHRs require certification, we would need a careful consideration of what criteria, due process, and skill set would be suitable. We believe that

there needs to be a thorough discussion about the pros and cons of various certification entities and a process to allow for competition among possible certification services.

In summary, we agree that solutions to privacy, security, and interoperability problems are needed to advance PHR adoption in this country. However, it is not warranted to assume that PHR certification is going to solve these issues or enhance consumer trust in PHRs. Credibility with consumers is a far different matter than credibility with vendors. Government encouragement of PHRs requires a public process that builds consumer understanding of the benefits of PHRs and confidence in the policies that underpin them. This requires a robust public debate on how privacy will be protected and secondary use controlled, and sustained public exposure to the benefits of PHRs and their role in their health and health care. What is needed now is for that discussion to take place, including a broader set of consumer representatives and industry experts, for a full exploration of these issues as well as the potential benefits, costs and risks of certification and its many alternatives. **For the reasons stated above, we believe it is premature for AHIC to adopt a recommendation on certification of PHRs and urge the Community to reject this recommendation.**

Sincerely,

Stephen Downs, The Robert Wood Johnson Foundation

David Lansky, Markle Foundation

JP Little, RxHub

Steve Shihadeh, Microsoft

Myrl Weinberg, National Health Council