# PHR Quandary: Despite the Benefits, Issues of Technology and Trust Slow Adoption

*by Harry B. Rhodes, MBA, RHIA, CHPS, CPHIMS*

Despite the proliferation of personal health record (PHR) technologies and services, only a small portion of the population uses them.[1] Indeed, some observers have expressed concern that PHRs will never catch on with the general public.[2] Yet when surveyed, consumers remain enthused about the possible benefits of the PHR.[3] Why are PHRs slow to catch on? The issues have to do with both technology and trust.

## Defining What a PHR Is and Isn't

One basic barrier to adoption is confusion about what a PHR is and isn't. The PHR is still being defined. *Personal health record* is a widely used but loosely defined term for a variety of emerging technologies that enable people to manage their health information and healthcare transactions electronically.

AHIMA defines the record as a lifelong resource owned and managed by the individual, secure and private, with the individual determining rights of access; it is separate from and does not replace the legal record of the provider.[4] The Connecting for Health Personal Health Working Group describes seven attributes of an ideal PHR:

1. Each person controls his or her own PHR.
2. PHRs contain information from one's entire lifetime.
3. PHRs contain information from all healthcare providers.
4. PHRs are accessible from any place at anytime.
5. PHRs are private and secure.
6. PHRs are transparent. Individuals can see who entered each piece of data, where it was transferred from, and who has viewed it.
7. PHRs permit easy exchange of information across health care systems.[5]

A quick review of these attributes against the present PHR environment reveals that the majority of current PHR applications lack the key functional attributes that would allow for networked health information exchange. Since many of the current PHR offerings are proprietary or simple in design, they lack the functionality to allow for universal access, exchange, and tracking of personal health information.

Many current electronic PHR offerings are just one evolutionary step up from paper medical files. The electronic health information documents contained within electronic PHRs have limited functionality. The documents are searchable, accessible, and printable within the host PHR application, but lack the interoperability, data integrity, and security functionality required for widespread network exchange.

## Reaping PHR Network Benefits

What is still missing from the PHR equation is the ability to network PHRs with healthcare providers' information systems. A networked environment for PHRs would serve as a foundation to improve health information exchange and as a result would improve the quality, affordability, and safety of care. A networked environment would allow enhanced communication between patients and providers and provide new tools to better manage personal healthcare and the healthcare of loved ones.

Connecting for Health notes that "the emergence of a networked electronic health information environment will transform patient care and improve the efficiency and effectiveness of the health system. At the same time, the emerging electronic health information infrastructure and the massive increase in the volume of health data that is easily collected, linked, and disseminated create unprecedented privacy and security risks that need to be adequately and appropriately addressed."[6]

Additionally, "These principles and the policies that flow from them promote balance between consumer control of and access to health information and the operational need to ensure that information uses and disclosures are not overly restricted such that consumers would be denied many of the benefits and improvements that information technology can bring to the health care system."[7]

Strong evidence indicates that healthcare consumers and providers would support a network for health information exchange-if security and confidentiality safeguards are sufficient.[8]

## Gaining Trust in PHRs

A functionally simple PHR maintained by a patient is valuable and would be trusted and accepted by healthcare providers who are familiar with the patient and have developed a relationship. However, few patients have long-term relationships with their healthcare providers.

Trust becomes an issue when providers are asked to accept PHR information at face value. In the absence of an established relationship between the provider and patient, the existence of security administration functionality will provide the assurance that the data within the PHR are trustworthy and have not been altered.

The inability to overcome the security, confidentiality, and data integrity functionality barriers has slowed the evolution of a networked PHR health information exchange. Healthcare providers and payers, fearing data integrity and reliability issues, have blocked PHR data exchange initiatives because of concerns about the extent to which patients should be able to change the content of their health records.

If patients have the ability to change the clinical information in their own records, physicians might deem the record unreliable. Payers, fearing possible insurance fraud or identity theft, are concerned about the validity of the information contained within the PHR. Consumers must have the ability to amend content without altering the orginal entry. If PHR data are required to adhere to the same security standards as EHR data, then they could be trusted.

Healthcare consumers' concerns have centered on knowing who has access to their data and why. Finally, reported thefts of laptops and systems security breaches have convinced many that system administrators are unable to adequately protect sensitive information.

## Creating Consensus

Before we set out to create a nationwide health information network that would connect the information in PHRs to other health information systems, we must come to agreement on a common set of shared rules, principles, and standards. We need a technical approach that allows access controls to keep information flowing among people authorized to see it and protected from unauthorized access or use. The selection and implementation of system audit technical elements can be aids or obstacles to confidentiality and security.

Many are calling for a health information exchange network that mirrors banking and financial networks. However, healthcare information is in many ways less structured, more complex, and more sensitive than financial data.

Our PHR network initiatives must be guided by a clear set of principles, and the Personal Health Technology Council, a collaborative body convened by the Markle Foundation, has offered a set of consumer- and patient-focused principles for the handling of electronic personal health information. The principles have been endorsed by many consumer groups and recommended to the American Health Information Community, an advisory body on health IT issues to the Department of Health and Human Services.[9,10,11]

The principles are:

- Individuals should be guaranteed access to their own health information.
- Individuals should be able to access their personally identifiable health information conveniently and affordably.

- Individuals should know how their personally identifiable health information may be used and who has access to it.
- Individuals should have control over whether and how their personally identifiable health information is shared.
- Systems for health information exchange must protect the integrity, security, and confidentiality of an individual's information.

Health IT vendors generally are reluctant to invest in the development of PHR network security, auditing, and privacy architecture where no clear standard or mandate exists. This poses another barrier to the creation of a viable and sustainable PHR network. The establishment of industry-recognized PHR networking architecture standards would do much to mitigate concerns and encourage vendor investment.

Fear of possible product liability also acts as a barrier to the development of PHR networking architecture. An established method of system application validation and certification would reduce concerns about reliability of security solutions.

## The Broad View

Currently available PHR applications operate as data silos, their lack of interoperability with other systems preventing the ready exchange of health information between systems. For PHRs to reach their true value they must allow for the secure and convenient interaction with multiple, disparate health data sources. The data in them must be traceable, so that each piece of content can be tracked from the point of its creation onward. Awareness of and compliance with standardized audit functionality would address the issues of trust and reliability.

Electronic health records are maturing, and much of the important pieces of consumer records already exist in a digital format. We must act now to address the security administration of these evolving systems. Consumers must be involved in the development of security technical and policy solutions to ensure the successful transition from the current state to a trusted network architecture designed to enable interoperable exchange.

## Notes

1. National Committee on Vital and Health Statistics. Letter to Secretary Leavitt on Personal Health Record (PHR) Systems. September 9, 2005. Available online at www.ncvhs.hhs.gov/050909lt.htm.
2. Tang, Paul, et al. "Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption." *Journal of the American Medical Informatics Association* 13, no. 2 (March–April 2006): 121–26.
3. Markle Foundation. "Attitudes of Americans Regarding Personal Health Records and Nationwide Electronic Health Information Exchange." October 2005. Available online at www.connectingforhealth.org/resources/101105_survey_summary.pdf.
4. AHIMA. "Defining the Personal Health Record." *Journal of AHIMA* 76, no. 6 (June 2005): 24–25.
5. Connecting for Health. "A Common Framework for Networked Personal Health Information." December 2006. Available online at www.connectingforhealth.org/commonframework/docs/P9_NetworkedPHRs.pdf.
6. Connecting for Health. "Model Privacy Policies and Procedures for Health Information Exchange." April 2006. Available online at www.connectingforhealth.org/commonframework/docs/P2_Model_PrivPol.pdf.
7. Ibid.
8. Markle Foundation. "Attitudes of Americans Regarding Personal Health Records and Nationwide Electronic Health Information Exchange."
9. Markle Foundation. "Electronic Health Data Exchanges: Patient and Consumer Principles for System Design." Available online at www.markle.org/downloadable_assets/consumer_principles_101105.pdf.
10. Personal Health Technology Council. Letter to Secretary Leavitt. March 6, 2006. Available online at www.connectingforhealth.org/resources/AHIC_Principles_PHTC_Letter.pdf.
11. Consumer Empowerment Working Group. Report to American Health Information Community. March 7, 2006. Available online at www.hhs.gov/healthit/documents/ AHICMarchNotebook.pdf.

***Harry B. Rhodes*** *(harry.rhodes@ahima.org) is director of practice leadership at AHIMA.*

**Article citation**:
Rhodes, Harry B.. "PHR Quandary: Despite the Benefits, Issues of Technology and Trust Slow

Adoption" *Journal of AHIMA* 78, no.4 (April 2007): 66-67;69.