INFORMATICS PROFESSIONALS. LEADING THE WAY.

December 10, 2010

Ms. Joy Pritts, JD
Office of the National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
200 Independence Avenue S.W.
Suite 729-D
Washington, D.C. 20201

Re: Request for Comments Personal Health Records (PHRs)

Dear Ms. Pritts,

On behalf of AMIA, I am pleased to submit these comments to inform your deliberations regarding the use of personal health records (PHRs). The questions you are considering are of great interest to AMIA, which is the leading professional association for the nation's top biomedical and health informaticians and serves as the center of action for the field as well as our members' unbiased and authoritative policy voice. Our 4,000 constituents play important roles in medicine, healthcare, and science, and encourage the use of data, information and knowledge to improve both human health and the delivery of healthcare services. Our members are an interdisciplinary and diverse group of individuals and organizations that come from numerous countries, organizations, and backgrounds, working to support and leverage basic and applied informatics principles to help inform public policy issues, such as research and evaluation, patient safety, technology, change implementation, and quality of care.

As you requested, we have organized our comments to respond to each of your overarching topics and related questions. Because of this formatting, some of our responses overlap as they are applicable to more than one topic.

Our comments are based on the following principles:

- The PHR is a tool or suite of tools for collecting, tracking and sharing important, up-to-date information about an individual's health or the health of someone in their care.
- Using a PHR will help people to make better health decisions and improve quality of care by allowing them to access and use information needed to communicate effectively with others about their healthcare.
- Empowering individuals to manage their healthcare better can in part be accomplished through the use of a PHR.

- Health information privacy and security protections must follow the personal health information (PHI) no matter where the data reside.
- All people are ultimately responsible for making decisions about their own health.
- All people should have access to their complete health information. Ideally, this information should be consolidated in a comprehensive record.
- Information in the PHR should be understandable to the individual.
- Information in the PHR should be accurate, reliable, and complete.
- All people should have control over how their PHR information is used and shared.
- Entities that operate/maintain a PHR and/or aggregate PHI data must be accountable to the individual consumer for unauthorized use or disclosure of PHI.
- A PHR may be separate from, and does not replace, the legal medical record of any provider.

Privacy and Security and Emerging Technologies. What privacy and security risks, concerns, and benefits arise from the current state and emerging business models of PHRs and related emerging technologies built around the collection and use of consumer health information, including mobile technologies and social networking?

AMIA recognizes and seeks to promote the benefits of patient-generated information for managing chronic illness and engaging patients and providers in shared decision-making. We believe that individuals should be able to readily access, understand, and use their PHI. Use of PHRs can allow individuals to be more active partners in their healthcare, and gives them up-to-date information when and where they need it. PHRs can provide a detailed and comprehensive profile of a person's health status and healthcare activity. It facilitates informed decisions about the care of the individual. PHRs also can help people to prepare for appointments, facilitate care in emergency situations, and help to track health changes. Currently, PHRs are available in multiple technologies (such as the web, patient portals, stand alone and integrated software packages) and via various technologies (such as PCs, mobile devices, and other digital devices).

In addition, there are a number of definitions for the term PHR, which may need to be reconciled and refined, especially as PHR technology and approaches evolve. For example,

- **HITECH, Sec. 13400:** The definition of Personal Health Record.—The term ''personal health record'' means an electronic record of personally identifiable health information (as defined in section 13407(f)(2)) on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual. (http://www.hipaasurvivalguide.com/hitech-act-13400.php#personal-health-record).

- **Centers for Medicare and Medicaid Services (CMS):** In general, a Personal Health Record (PHR) is controlled by the individual, and can be shared with others, including caregivers, family members and providers. This is different from a provider's electronic health record, which is controlled by the provider just as paper medical records are today. Ideally, a Personal Health Record will have a fairly complete summary of an individual's health and medical history based on data from many sources, including information entered by the individual (e.g., allergies, over-the-counter medications, family history, etc.). (http://www.cms.gov/PerHealthRecords/01_Overview.asp).

- **Federal Trade Commission (FTC):** In general, personal health records are online repositories of health information that individuals can create to track their medical visits, and prescription information, etc. (FTC Health Breach Notification Final Rule - http://edocket.access.gpo.gov/2009/pdf/E9-20142.pdf).

Regarding privacy and security, we believe that consumers (users) of PHRs should be provided with the following information:

- Identity of the PHR provider/operator/aggregator and means to contact the provider.

- Policies of the PHR provider/operator/aggregator on security, privacy and data ownership.

- The source(s) of specific data in the PHR; in particular, it is important to distinguish data entered by a consumer from data entered by a healthcare provider.

- A record of which individuals or entities have viewed, modified, or transmitted data from the PHR, when such actions occurred, and what data were viewed, modified, or transmitted.

AMIA is concerned that in the absence of clear Federal guidance and/or regulations, PHRs operated or maintained outside of a direct care delivery system, which are not subject to HIPAA, may introduce privacy and security harms to consumers. The current lack of coherent regulations, legislation, and/or policies and procedures for PHRs presents significant challenges for consumers. Some of the resulting questions that accordingly arise from observers or consumers are:

- What are the potential benefits and risks regarding the development, maintenance and use of PHRs?

- Who has the right to access the data and for what purposes?

- What are the evolving public trust issues with respect to PHRs?

- What challenges may develop as innovative technologies enhance the ability and ease of widespread creation and maintenance of PHRs?

- What is the potential for inappropriate use and/or exploitation of PHR data?

AMIA supports the efforts of the Office of the National Coordinator (ONC) to collaborate with other Federal agencies such as the FTC and the Office of Civil Rights (OCR) to undertake additional efforts that will establish consistent policies and regulations to address consumer protections in this area. With appropriate technical safeguards and supportive public policy, AMIA believes that the use of PHRs can further the public good.

Consumer Expectations about Collection and Use of Health Information. Are there commonly understood or recognized consumer expectations and attitudes about the collection and use of their health information when they participate in PHRs and related technologies? Is there empirical data that allows us reliably to measure any such consumer expectations? What, if any, legal protections do consumers expect apply to their personal health information when they conduct online searches, respond to surveys or quizzes, seek medical advice online, participate in chat groups or health networks, or otherwise? How determinative should consumer expectations be in developing policies about privacy and security?

AMIA questions whether consumers fully understand or appreciate the magnitude of both the potential advantages and the risks associated with PHR data. We believe that consumers who use a PHR and other health-related online web sites typically do so because they or a family member have a personal health-related information need or questions for which they seek answers. In such instances, their focus is not on protecting privacy but rather on obtaining needed information.

Consumers need to be better educated about the privacy and security policies and procedures employed by entities that manage PHRs and other health-related online services to make sure they understand how their personal health information is used and protected. Education can address the ability of the individual, or those they authorize, to access their information, and the ability of the individual to control use of PHR data by others.

AMIA believes that further educational efforts are needed related to the following issues:

- Consumers may not understand the types of products available and the differences among classes of PHRs (e.g., provider-managed vs. commercial).

- Consumers may not understand what components or technologies are needed to ensure the confidentiality, privacy and security of their personal information.

- Consumers may not recognize when their own uses of social networking and mobile technologies result in unintended release of personal information they wish to keep private.

- Consumers may not be able to determine whether implemented security technologies and privacy policies are adequate to ensure the security and privacy they expect.

- Consumers may not be able to recognize policy violations and security breaches resulting in threats to their privacy.

- Consumers may not understand how to seek correction of security-related problems and redress for material harms resulting from security breaches.

- Consumers may not know if the providers' EHR is interoperable with the consumer's PHR system. A clear understanding is required in order to determine fully the healthcare related benefits and limitations.

Because we believe that the value of a PHR increases with its ability to incorporate data from other systems and to transmit data to other systems, efforts to develop standards for semantic interoperability between PHRs and other clinical information systems should be supported. This approach is consistent with the recent President's Council of Advisors on Science and Technology (PCAST) (http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-health-it-report.pdf) report entitled, *Realizing the Full Potential of Health Information Technology to Improve Healthcare for Americans: The Path Forward*. The report noted that "to date most PHRs are not standards based, and few support an easy way to transport records among different EHR products."

AMIA is concerned that the current security and privacy practices developed under HIPAA guidelines are not applicable to the development and use of all PHRs. Having long argued for the establishment of a chain of trust for uses/disclosures of PHI, we believe that entities that receive, transmit, disclose or use PHI (including for use in PHRs) should indeed follow the Privacy Rule requirements for use and disclosure and should have security measures in place in order to keep such information confidential. AMIA supports the extension of HIPAA rule compliance obligations to PHR vendors.

CMS requires that "Health plans and most healthcare providers who offer PHRs must give you a Notice of Privacy Practices, which tells you how they keep your personal information private and safe (http://www.medicare.gov/Publications/Pubs/pdf/11397.pdf)". AMIA believes that PHRs offered by others (such as commercial entities and health insurance companies) should be governed by similar requirements. Additionally, AMIA proposes that other concerns warrant ONC and FTC attention, such as:

- There is a lack of commonly understood or recognized consumer expectations and attitudes about the collection and use of their health information when they participate in PHRs and related technologies.

- There is a need to clarify the extent to which current policies and legislation afford sufficient protections and address issues related to the privacy and security of consumers' personal health information within PHRs.

- Further, it is not clear if or how current policies address personal health information privacy and security when consumers conduct online searches, respond to surveys or quizzes, seek medical advice online, or otherwise participate in chat groups or health networks.

- It is not clear how the current concepts of privacy and security relate to the implementation and growing use of social networking approaches and applications for PHRs.

AMIA believes that consumer expectations must be considered when developing policies about PHR privacy and security. Policies that consumers feel benefit commercial interests rather than consumers' interests are unlikely to facilitate consumer trust.

AMIA notes that Project HealthDesign grantees, and other groups such as Pew and Kaiser (see for example, http://www.pewinternet.org/Reports/2010/Future-of-the-Internet-IV.aspx) are a rich source of data about consumer expectations and attitudes regarding PHRs. Testimony by Dr. Patti Brennan to the Meaningful Use Workgroup in April 20, 2010 (see http://healthit.hhs.gov/portal/server.pt?open=512&objID=1472&&PageID=17094&mode=2&in_hi_userid=11673&cached=true) indicates that consumers with chronic conditions expect their health information to be available in a computable form that allows them to see patterns and trends (e.g., the relationship of physical activity and diet changes to weight loss), and that allows them to interact with their own information.

AMIA believes that consumers should be full participants in the development and implementation of policies that are clearly defined and written in plain language that is easily comprehensible to the average consumer. The freedom of consumers to choose whether to use a PHR should not be infringed. The use of a PHR should not be required as a condition of health insurance coverage or employment. Consumers have a right to access all of their data in a PHR. If the status of a patient as a user of a PHR terminates, the patient should have the right to receive a copy of their PHR data in a form that is human-readable or can be rendered human-readable with commonly available applications.

- Both the functionality and content of PHRs should be understandable to the consumers who use them.

- Systems should be consciously designed for users with varying levels of health literacy. This will not only help consumers understand the information presented to them; it will also make it less likely they will enter information that is erroneous or liable to misinterpretation by health care personnel.

- Efforts should be undertaken to map health care terminologies to lay terms so that information can be presented in a comprehensible form to consumers.

- PHRs should make it clear to users whether or not another person or entity (for instance, a healthcare provider), will be alerted to data they have entered or modified. This can avoid situations where a patient believes such communication will occur when, in fact, it will not.

- PHRs should make very clear to consumers the consequences of control decisions (i.e., the possible consequences of authorizing or withholding permission for other entities to access their data).

Privacy and Security Requirements for Non-Covered Entities. What are the pros and cons of applying different privacy and security requirements to non-covered entities, including PHRs, mobile technologies, and social networking?

Non-covered entities must be held to the same privacy and security requirements as covered entities in order for consumers to be assured of privacy and security of their PHI. Without this accountability, consumers may lose their trust in non-covered entities, thereby reducing use of PHRs, mobile technologies, and other health-related social networking tools. In the event that non-covered entities are not held to the same privacy and security requirements as providers and other covered entities, some consumers may determine that the benefits of using these technologies outweigh the risks associated with the less stringent requirements, but some likely will not and will thereby lose the potential benefits resulting from PHR use.

There may be a benefit in having tiered access to information that is more sensitive and can be protected and accessed only by approved individuals and organizations, while information that may be more broadly useful and less sensitive may be made more generally available provided that the consumer wants to share it. One challenge given existing rules and regulations is how to administer different privacy protections across technologies or platforms. One way to mitigate the administrative challenges is to have fully informed consumers who give explicit permission and/or opt-in in response to explanations of how their personal health information might be used or who might see it.

To accelerate the adoption of PHRs, and to ensure that minimum requirements for functionality, security, and interoperability are met, a certification process for PHRs would be beneficial. Such a process should be based on needs as defined by appropriate stakeholders, and not impose undue constraints on innovation.

The benefits of PHRs are to some degree speculative. Therefore, PHRs should be studied more thoroughly to evaluate their effectiveness and to determine how they can be designed and implemented to achieve their expected benefits.

AMIA also suggests further study in the following areas:

- Increased potential for identity theft as PHRs become commonplace.
- Increased potential for healthcare fraud.

Any other Comments on PHRs and Non-Covered Entities. Do you have other comments or concerns regarding PHRs and other non-covered entities?

AMIA is concerned about the lack of transparency for non-covered entities that operate or maintain PHRs. There is a need for consumers to be explicitly informed about the privacy and security practices employed by those who operate or maintain PHRs.

AMIA emphasizes the need for further development of policies, rules and/or regulations to direct and monitor the use of personal health information maintained/stored within PHRs and related technologies and applications. For example, AMIA believes that ONC needs to explore the evolving use of "web 2.0" applications and their potential relationship to PHRs. AMIA believes that policies should address the use of personal health information contained within such applications. AMIA also believes that additional study, research and evaluation is needed to address the potential policy issues related to the evolving use of various mobile technologies and devices and web-based portals and tools that collect or use PHI. Technology is advancing faster than the policies that govern them.

Summary

On behalf of AMIA, I would like to thank the ONC for focusing attention on an important public policy issue. As a source of informed, unbiased opinions on policy issues relating to the national health information infrastructure, the uses and protection of clinical and personal health information, and a variety of public health considerations, AMIA appreciates the opportunity to contribute to your deliberations. Finally, AMIA again wishes to thank you for convening the PHR Roundtable and for inviting public comments and testimony. We have appended a list of selected relevant resources for your consideration. Again, please feel free to contact us at any time for further clarification of the issues we have raised.

Sincerely,

Edward H. Shortliffe, MD, PhD
President and CEO

Selected References

Bates DW, Bitton A. The future of health information technology in the patient-centered medical home. Health Aff (Millwood). 2010 Apr;29(4):614-21.

Bloomrosen M, Detmer D. Advancing the framework: use of health data--a report of a working conference of the American Medical Informatics Association. J Am Med Inform Assoc. 2008 Nov-Dec;15(6):715-22. Epub 2008 Aug 28.

Bloomrosen M, Detmer DE. Informatics, evidence-based care, and research; implications for national policy: a report of an American Medical Informatics Association health policy conference. J Am Med Inform Assoc. 2010 Mar-Apr;17(2):115

Brennan PF, Downs S, Casper G. Project HealthDesign: rethinking the power and potential of personal health records. J Biomed Inform. 2010 Oct;43(5 Suppl):S3-5.

Cushman R, Froomkin AM, Cava A, Abril P, Goodman KW. Ethical, legal and social issues for personal health records and applications. J Biomed Inform. 2010 Oct;43(5 Suppl):S51-5.PMID: 20937485 [PubMed - in process].

Goodman KW, Berner ES, Dente MA, Kaplan B, Koppel R, Rucker D, Sands DZ, Winkelstein P; for the AMIA Board of Directors. Challenges in ethics, safety, best practices, and oversight regarding HIT vendors, their customers, and patients: a report of an AMIA special task force. J Am Med Inform Assoc. 2010 Nov 12. [Epub ahead of print]

Khaled El Emam, Emilio Neri, Elizabeth Jonker, Marina Sokolova, Liam Peyton, Angelica Neisa, Teresa Scassa. The inadvertent disclosure of personal health information through peer-to-peer file sharing programs JAMIA 2010;17:148-158.

Patti Brennan, University of Wisconsin, Project HealthDesign Testimony to Meaningful Use Workgroup, Patient/Consumer Engagement Hearing, April 10, 2010. http://healthit.hhs.gov/portal/server.pt?open=512&objID=1472&&PageID=17094&mode=2&in_hi_userid=11673&cached=true.

Project Health Design: http://www.projecthealthdesign.org/

Raymond B, Tang P. Integrated personal health records: transformative tools for consumer-centric care.BMC Med Inform Decis Mak. 2008 Oct 6;8:45.

Roblin DW, Houston TK 2nd, Allison JJ, Joski PJ, Becker ER. Disparities in use of a personal health record in a managed care organization. J Am Med Inform Assoc. 2009 Sep-Oct;16(5):683-9. Epub 2009 Jun 30.

Simborg DW. Consumer empowerment versus consumer populism in healthcare IT. J Am Med Inform Assoc. 2010 Jul-Aug;17(4):370-2.

Sujansky WV, Faus SA, Stone E, Brennan PF.A method to implement fine-grained access control for personal health records through standard relational database queries. J Biomed Inform. 2010 Oct;43(5 Suppl):S46-50. Epub 2010 Aug 7.

Safran C, Bloomrosen M, Hammond WE, Labkoff S, Markel-Fox S, Tang PC, Detmer DE, Expert Panel. Toward a national framework for the secondary use of health data: an American Medical Informatics Association White Paper. J Am Med Inform Assoc. 2007 Jan-Feb;14(1):1-9. Epub 2006 Oct 31.

Statement on Health Information Confidentiality. A Joint Position Statement for Consumers of Health Care by the American Health Information Management Association (AHIMA) and the American Medical Informatics Association (AMIA) July 2006 https://www.amia.org/files/amia_ahimajointconfidentialitystatement.pdf.

Tang PC, Lee TH. Your doctor's office or the Internet? Two paths to personal health records. N Engl J Med. 2009 Mar 26;360(13):1276-8. .

The Value of Personal Health Records. A Joint Position Statement for Consumers of Health Care by the American Health Information Management Association (AHIMA) and the American Medical Informatics Association (AMIA) July 2006 https://www.amia.org/files/ahima-amiaphrstatement.pdf Accessed 12/06./10.

Weitzman ER, Kaci L, Mandl KD. Sharing medical data for health research: the early personal health record experience. J Med Internet Res. 2010 May 25;12(2):e14.