

December 1, 2010

David Blumenthal, MD, MPP  
National Coordinator for Health Information Technology  
Department of Health and Human Services  
Submitted electronically

Re: Personal Health Records

Dear Dr. Blumenthal:

The College of Healthcare Information Management Executives (CHIME) appreciates the opportunity to respond to the request for input regarding personal health records (PHRs). As we understand it, this request for comments is intended to help inform a report to Congressional committees of jurisdiction that is mandated by section 13424(b) of the Health Information Technology for Economic and Clinical Health Act (HITECH Act). This report must address privacy and security requirements for entities that were not covered entities or business associates as of February 17, 2009, including vendors of PHRs and a range of entities that interact with PHRs.

CHIME's 1,400 members represent chief information officers (CIOs) and other top information technology executives at many of the nation's largest hospitals. CHIME members have front-line experience in implementing clinical systems, and have learned by trial and error what works and what doesn't in implementing such electronic systems and optimizing the value derived from them. Healthcare CIOs share the vision of an e-enabled healthcare system as described by the HIT Policy Committee, the Office of the National Coordinator for HIT, and the Centers for Medicare & Medicaid Services.

### **Making PHR Vendors Directly Accountable**

CHIME believes that the most important thing that could be done to adequately protect PHR users would be to make PHR vendors directly accountable for meeting the privacy and security requirements under the Health Insurance Portability and Accountability Act (HIPAA), including breach notification requirements. This could be accomplished by making such vendors HIPAA-covered entities or an alternative that would have the same result. We believe this would be better than other approaches, such as through business associate agreements with HIPAA covered entities or other less direct means. We recognize, of course, that a proposed rule published on July 14, 2010 by the Office for Civil Rights of the Department of Health and Human Services (HHS) proposed, among many other things,

that the term “business associate” include “a person who offers a personal health record to one or more individuals on behalf of a covered entity.” Nevertheless, we believe that the vulnerabilities inherent in PHR functions, including receipt of protected health information, serving as repositories of such information, and exchanging such information with others, necessitate a clear delineation of PHR vendor obligations. Otherwise, we fear that users of PHRs will not be adequately protected or that covered entities that interact with PHRs will inappropriately incur responsibilities that are not theirs.

### **Standardizing Exchanges between PHRs and Others**

In addition to making PHR vendors directly responsible for meeting privacy and security requirements, we also believe it would be important for information exchanges between PHRs and others to be standardized to the greatest extent possible. Thus, rather than having each PHR vendor adopt unique ways to receive information from, and transmit information to, a HIPAA covered entity, we believe that such transactions should occur in a standardized fashion. Such standardization would help ensure that information exchanges are efficient and accurate, and would also facilitate privacy and security protections.

CHIME’s members also wish to be able to accept information from a PHR “as is.” For example, if an individual patient or consumer wishes to protect some aspect of the information in his or her PHR in a special way, we believe it should be the obligation of the PHR vendor to remove such information prior to any sharing of the contents of an individual’s PHR with a hospital, physician or other person.

### **Liability Concerns**

CHIME members are concerned about the potential liability exposure that can arise when information flows to and from PHRs. For example, we are concerned that information transmitted to a PHR from a hospital might subsequently be altered. We are also concerned that information received from a PHR by a hospital might be inaccurate or incomplete, potentially compromising safe, effective and efficient patient care. For this reason, some of our members have taken steps to designate information received from a PHR as “external” information and even place it in a separate area of a patient’s electronic health record (EHR), in order to distinguish this information from other information generated by the hospital itself or by clinicians caring for the patient in the hospital.

All of these liability concerns lead us to conclude that hospitals should not be required to create PHRs or to have any particular relationship with PHR vendors (for example, as part of any meaningful use requirements). Instead, any PHR-related interactions involving a hospital should remain voluntary and should obviously occur only with a patient’s explicit authorization. We also ask that HHS remain sensitive to our liability concerns as you make recommendations relating to PHRs, including those addressing privacy and security matters.

## **The Value of Unique Patient Identifiers**

Lastly, CHIME continues to believe that a unique patient identifier would have great value and facilitate the efficient and accurate electronic exchange of information between all relevant parties, including PHR vendors. We appreciate the sensitivities involved with such identifiers but we also are concerned that the alternative methodologies currently in place do not provide absolute assurances that information about a patient will be sent to the right patient's EHR or PHR. Thus, we wish to use this opportunity to again voice our support for unique patient identifiers.

We hope these comments are helpful. If you have any questions about our comments or need more information, please contact Sharon Canner at [scanner@cio-chime.org](mailto:scanner@cio-chime.org).

Sincerely,

A handwritten signature in black ink, appearing to read 'R. Correll', with a long horizontal flourish extending to the right.

Richard A. Correll, President & CEO