American Health Information Management Association (AHIMA)
Written and Oral Testimony at the
NCVHS Privacy, Confidentiality and Security Subcommittee
Hearing on Personal Health Records

May 20, 2009

Submitted by:
Donald T. Mon, PhD
Vice President, Practice Leadership

As a volunteer to the standards development efforts at HL7, Dr. Mon is:

- **A member of the Board of Directors**
- **Co-Chair of the EHR Work Group that developed the fully ANSI accredited EHR System Functional Model (EHR-S FM) and sponsors PHR activities within HL7**
- **Co-Facilitator of the PHR WG that developed the PHR-System Functional Model (PHR-S FM) Draft Standard for Trial Use**

Dr. Mon has also served on the following industry PHR activities:

- **CCHIT PHR Advisory Task Force (Commissioner-level responsibility) that provided direction for PHR certification**
- **Expert Panel, Evaluation of CMS PHR Pilot Projects (ASPE sponsored study)**
- **Co-chair, Key Definitions of the EMR, EHR, and PHR Work Group, a National Alliance for Health Information Technology (NAHIT) project funded by ONC**

About AHIMA

AHIMA is a not-for-profit professional association representing more than 53,000 health information management (HIM) professionals who work throughout the health care industry. AHIMA's HIM professionals are educated, trained and certified to serve the health care industry and the public by managing, analyzing, reporting, and using data vital for patient care, while making it accessible to health care providers and researchers.

The AHIMA Foundation is the charitable affiliate of AHIMA which provides financial and intellectual resources to sustain and recognize continuous innovation and advances in HIM for the betterment of the profession, health care, and the public.

In addition to the EHR, the PHR, and health information exchange (HIE), AHIMA and its members participate in a variety of projects with other industry groups and federal agencies regarding the use of health care data for direct care, quality measurement, reimbursement, public health, patient safety, biosurveillance and research.

AHIMA
American Health Information
Management Association®

American Health Information Management Association (AHIMA)
Written and Oral Testimony at the
NCVHS Privacy, Confidentiality and Security Subcommittee
Hearing on Personal Health Records

May 20, 2009

Submitted by:
Donald T. Mon, PhD
Vice President, Practice Leadership

Opening Comments

Good morning, co-chairs Houston and Francis, members of the Privacy, Confidentiality and Security Subcommittee, and fellow participants. My name is Donald Mon, vice president for practice leadership at the American Health Information Management Association (AHIMA). AHIMA is a society of 53,000 health information management professionals who manage health records across all healthcare settings.

We appreciate the opportunity to respond to the following questions forwarded to us by the staff of this subcommittee:

- What is the problem PHRs are trying to solve today?
- How do you envision the relationships among PHRs, electronic health records, providers, plans, health information exchanges, etc. evolving over the next five or ten years?
- How do you see the development of health IT, and PHRs in particular, incorporating individual participation now, and in the future?
- To what extent do you think there will be "uptake" for PHRs or other patient-facing online services and why?
- To what extent do you expect PHRs to be a “source record” for medical information?
- What kinds of privacy, security, and confidentiality issues, do you think consumer-focused health IT, and PHRs in particular, will have to grapple with in the coming years?

Our responses to the above questions are based on two sets of experiences:

- Our engagement with consumers through our consumer-oriented PHR website (www.myPHR.com), consumer education program, and media campaign
- Our participation in industry initiatives focused on defining the PHR and distinguishing it from the EHR, developing PHR system standards, certifying PHR systems, and evaluating PHR demonstration projects

In our responses, we have referenced, but not reiterated, the findings in the literature. In addition, we have avoided comments that we expect other invited participants will provide today. The major themes in our responses are health information management practices and principles, and the current state and future direction of PHR standards, especially as they relate to privacy, confidentiality and security.

Responses to Questions

What is the problem PHRs are trying to solve?

"What problems PHRs are trying to solve" is exactly the right question to ask when setting direction for PHR initiatives. Getting clarity on this question will reduce the confusion the industry is experiencing in defining the PHR and distinguishing it from the EHR, setting PHR standards, developing PHR systems for the marketplace, identifying the PHR's role in exchanging health information with EHRs both directly and across health information exchanges (HIEs), and accelerating PHR adoption.

The practical problems PHRs are trying to solve are well documented and real. For example, using PHRs to provide physicians (1) with accurate doses of medications to prevent an order for a medication that is contraindicated (patient safety), or (2) with timely and accurate values to clinical tests to avoid duplication of tests (reduced cost), and so on, are true benefits PHRs can provide. AHIMA supports the consumer empowerment principle that PHRs can be used effectively to enable consumers to make informed health decisions, facilitate patient-clinician communication, provide convenience (e.g., scheduling appointments with the doctor) and exchange health information with providers, resulting in increases in quality care, reduced cost and a better healthcare experience for the patient.

How do you envision the relationships among PHRs, electronic health records, providers, plans, health information exchanges, etc. evolving over the next five or ten years?

The issue is not so much "what problems PHRs are trying to solve," as it is the role of the PHR as one of many, sometimes overlapping, health information technologies involved in the solutions to the problems. Some argue, for example, that there would be little need for PHRs if patient portals were widely available for consumers to maintain health information in their records and EHRs were interoperable enough to exchange health information with other EHRs, registries and repositories for other secondary data uses. While others argue that PHRs can be a less costly way to exchange health information with a provider's EHR than either direct EHR to EHR communication or through health information organizations (HIOs). Still others ask whether the primary purpose of PHRs should be to exchange health information or just serve as a record consumers keep for themselves.

The last is a valid question because a major stumbling block for the PHR occurs when it is used for health information exchange. At that point, the PHR is scrutinized as to whether it represents both the source of truth and the truth of source—issues I will be coming back to later in our response to the privacy, confidentiality and security question.

In looking at the evolving relationship among PHRs, EHR, HIE, physicians, health plans, etc. over the next decade, the industry has to consider that PHR systems, EHR systems, and health information organizations and the exchange process itself, all have low rates of adoption at this point and need much more time and investment to mature as a product, organization, or process. Yet, this state of affairs presents an opportunity to clarify the relationships among them, and identify how each has to evolve over the next few years to interact and grow in concert with each other.

One of the keys to this evolution is again the focus on health information exchange. EHR products installed well before the development of PHRs currently lack the ability to provide patient portals and exchange data with PHRs. Without the latter, the exchange of data between PHRs and EHRs will require manual entry for both systems, which will hinder PHR usage in hospitals and physician offices and in turn hinder PHR adoption. Therefore, one of the main thrusts over the next five years should be to build data exchange functionality into EHR systems so that as providers acquire, upgrade or replace their EHR systems they will be able to exchange data between their EHR and the patient's PHR. Similarly, PHR systems must be developed with reciprocal exchange functionality.

Exchanging data is not simply exporting and importing the Continuity of Care Document (CCD). Other important issues must be addressed. For example, the Health Level Seven (HL7) Electronic Health Record System Functional Model (EHR-S FM) and the Personal Health Record System Functional Model (PHR-S FM) point out that both systems must explicitly label the source of captured data in order to preserve the truth of source.

The longitudinal record, which could range as much as from birth to death, has long been a goal of both the EHR and the PHR. Provider-sponsored PHRs—the term used in the PHR-S FM, and called "tethered PHRs" or "tethered EHRs" in other places—are longitudinal to the degree that the consumer has received care from that provider over time. Some providers state that they intend to keep a patient's record in their EHR system for longer durations (e.g., 20 years, forever) than they have in the past. However, the industry does not have enough experience to know how long community hospitals and small doctor offices, abiding by their risk assessment and record retention/destruction policies, will really store records in their EHR system. The variability in record storage across provider-sponsored PHRs places more importance on the PHR to act as the consumer's longitudinal record.

It will be more important, then, that health information exchange between the PHR and the EHR occur at the end of each visit or encounter or as soon afterwards as possible. Should either the consumer or the provider wait until the provider states it will no longer keep the patient's record in its EHR system, then parts of, or perhaps even the entire, record for each visit or encounter may be transferred to the PHR. However, there is no industry proof at this time that the different EHR systems that may be present in multiple provider offices or hospitals can reliably exchange data with the PHR, where the latter can store the receiving information in its data fields.

How do you see the development of health IT, and PHRs in particular, incorporating individual participation now, and in the future?

Aside from privacy, confidentiality and security (addressed in a later response), convenience, making the interaction with the PHR an engaging experience, and increased non-healthcare functionality will be keys to incorporating individual participation. The convenience of auto-population may still serve as one of the most attractive features for PHRs over the next few years. An auto-populated PHR has been used as a way to maintain customer loyalty to the sponsor of the PHR. However, some consumers may be undeterred with their health information spread out over multiple places (e.g., provider-sponsored and payer-sponsored EHRs) just as they accept having their savings accounts, checking accounts, certificates of deposits, money markets, and retirement accounts distributed over multiple institutions. This type of functionality may make some PHRs attractive, particularly if the PHR system provides an engaging experience and other non-healthcare functionality. For example, just as Quicken or Microsoft Money pulls data from multiple sources and presents a view of net worth, PHR systems can provide a net health (the person's health status) view to the consumer. Imagine, too, PHR systems in the future submitting the bill, claim payment, and medical flexible spending form for reimbursement.

Note the nuance in the Quicken/Money example. Those systems pull the data into their respective databases so that it can produce charts of net worth increases or diminishes over time. Some have suggested that PHRs need not be the repository for health data, but merely point to the sources where the data actually resides and provide integrated views from those sources. That may be worthwhile functionality, but as pointed out earlier, providers may archive, purge, or destroy records at any given time. Consequently those records would not be available for other functions to use.

Cell phones and personal digital assistants (PDAs) have been mentioned recently as the next form factor (both application and device) for PHRs. While such devices may not have the storage to contain a longitudinal record, they certainly are sufficient for health information exchange with an EHR via Bluetooth or USB drive. This may soon be a reality as device manufacturers improve technology in this area. There is evidence that such movement is afoot. For example, one manufacturer of microdisks for cell phones has recently approached HL7 to work on device-level security.

To what extent do you think there will be "uptake" for PHRs or other patient-facing online services and why?

Uptake for PHRs and other patient facing online services, however, will continue to be slow over the next few years. In addition to the reasons cited in the literature, the factors highlighted in this testimony need to be addressed. These factors themselves require time and financial investment to develop or enhance PHR and EHR systems accordingly.

Each PHR model has its own limitations with respect to uptake. For example, given that EHR systems have been adopted by only a single digit or low double digit percentage of doctor’s offices and hospitals, and only a fraction of those systems have patient portals, it will take some time for provider-sponsored PHRs to proliferate.

However, as source of truth (trust) and truth of source, health information exchange between the EHR and the PHR, privacy, confidentiality and security, convenience, engaging customer experience, added PHR functionality, and other important issues are addressed, uptake will grow.

Uptake will greatly increase as a result of greater consumer education at two levels. First, there needs to be more consumer awareness campaigns (e.g., similar to what the Ad Council produces) so that consumers can at least begin to inquire about PHRs and its benefits. Second, there needs to be more education and support from providers, health information management professionals, and vendors to help consumers get started with their PHR and answer whatever questions they may have.

To what extent do you expect PHRs to be a “source record” for medical information?

AHIMA expects PHRs to be *a* source record, but perhaps not *the* source record at least for the foreseeable future. This situation will continue to exist as long as source of truth and truth of source issues and policies remain unresolved. Moreover, PHRs will increasingly be viewed as trusted source records as data quality and data integrity increases. While not completely exhaustive, there are a number of technical and functional standards that facilitate data quality and data integrity. Policy and standards, however, can only do so much. Data quality and data integrity also depends on the conscientiousness with which consumers capture data from external sources, enter patient-sourced data, and manage all that data in their PHRs.

What kinds of privacy, security, and confidentiality issues, do you think consumer-focused health IT, and PHRs in particular, will have to grapple with in the coming years?

The major privacy issue in front of the HL7 PHR Work Group is whether or not consumers should have the ability to modify professionally sourced data. In reality, this issue is tied to the larger issue of patients “withholding” information from their physicians, so both issues must be addressed. AHIMA’s stance on these privacy issues is that physicians need as much information as possible in order to provide the best care. Thus, patients should be encouraged to tell their physicians as much as they are comfortable with, and trust that the clinician will keep the information confidential. AHIMA encourages a balance between protecting the privacy of the individual and the confidentiality of the health information with the need to facilitate patient-clinician communication and the exchange of health information between EHRs and PHRs.

The issue of the consumer's ability to modify professionally sourced data is intertwined with two other factors: (1) "ownership of the data" where ownership is defined as having complete sovereignty over the data, and (2) the type of PHR model in question. In the second factor, it is important to distinguish between the personal health *information* that is stored in an underlying *record* and maintained by a *system* providing application-level functionality.

These two factors can help dissect and bring to resolution the longstanding debate surrounding the modification of professionally sourced data. On the one hand, advocates assert that the consumers "own the data" and therefore should have the right to do anything they want with it, including modifying professionally sourced data captured in their PHR systems. Others say that providers own the data and are bound to preserve the integrity of the data in order to maintain a legal record for business and disclosure purposes.

Here is how the two factors can shed light on the problem. In an EHR the patient cannot access the record and willfully make changes to professionally sourced data because the EHR is that provider's legal record for business and disclosure purposes and certain records management practices must be used accordingly. Thus, the patient must request that the change be made. If the provider agrees, he or she will (a) leave the original data in the record, (b) attach the request and note that the consumer has requested a change to the data, (c) add the requested change to the data, and (d) mark the changed data as an amendment (for augmentation, modification, append, etc.). If the provider disagrees, then he must note in the record that the request for the modification was made but denied, and state the reason for the denial.

This is important because the underlying record in the "tethered PHR" is the provider's EHR. Thus, in this model, the consumer does not have complete sovereignty over all the data, but can still exercise his or her privacy rights.

On the flipside, in non-provider sponsored PHR models, the underlying record is not an EHR, and therefore, not a legal record for business and disclosure purposes. In addition, the system maintaining the record sits outside the provider's enterprise (e.g., on a home computer, as an online service, etc.). Thus, from a practical standpoint, while it is desirable for PHR systems to contain the same records management functions to maintain the integrity of the data as with EHRs, there is no law requiring or standard of practice encouraging them to do so. In fact, it is difficult to conceive of consumers taking the rigor involved in managing the EHR and how consumers can be prevented from modifying professionally sourced data in non-provider sponsored PHR models.

A PHR system can be developed to literally prevent consumers from modifying professionally sourced data in non-provider sponsored PHRs. But then there is the risk that consumers will be frustrated and dissatisfied with the system and will stop using it, which in turn, hinders PHR adoption. With non-provider sponsored PHRs, the physician does not have complete sovereignty over the data.

It is important to bring out the differences highlighted by these two factors because the debate (or the confusion) in the industry around the modification of professionally sourced data appears as though all the same privacy rights, system functions, and standards should apply to all PHR models, when they don't.

As a side note, AHIMA encourages the industry to discontinue the use of the phrase "ownership of the data" because no single individual—whether the patient or the physician—has ever had complete sovereignty over the data. Further, the phrase injects emotion into the discussion and sets up unwarranted expectations. It is more accurate to state that the patient has within limits the right to determine (control) who can access and use the health information in the record—hence the phrase "access, use and control."

An important dimension in the discussion surrounding the consumer's ability to modify professionally sourced information is data integrity that can build physician trust. If the consumer modifies professionally sourced data with no audit record tracking the original state of the data, the changed state of the data, the person who modified the data, and when the data was modified, data integrity is compromised. Worse, physicians will not trust the data in the PHR, and not access it or rely on it even if accessed, rendering the PHR useless for health information exchange. At that point, the PHR will really be just the record consumers keep for themselves, if they do it at all once they see their physician's reaction to it.

In order to preserve data integrity and build trust in the data, some have argued that:

- Amended data is clearly flagged, showing also the source of the original data, and the original data itself
- Systems should not be able to receive amended data without also receiving the metadata indicating that a change was made and the source of the changes
- Amended data are always stored with received data and displayed conspicuously (the original data is not hidden in an audit trail requiring a busy physician to take the time to search for it)

If such data were true amendments where the patient and the physician interacted as in our example above, then these actions would adhere to excellent records management practices. However, if the data were modified by the consumer with no discussion with the physician, then showing the modified data alongside the original data, or even exposing the original data in an audit log, may disclose the very data the consumer wished to withhold.

Since there is no policy guiding the standards community in this regard, and since standards should not develop policy, the HL7 PHR WG has had to grapple with the balance between data integrity and privacy on this very issue. The PHR WG developed conformance criteria stating that at one level a flag should appear in the beginning of the record alerting the physician that something in the record was modified, but is not shown the original data which the consumer wished to withhold. This would allow the physician to assess the data as a source of truth and know whether to engage in a dialog with the patient about matters of trust, the need for accurate data, in addition to the patient's health.

At another level, the PHR WG is considering a criterion that simply changes the attribution of the data from the professional source to the patient at the time the modification was made, with no audit trail of the original data, the change to the data, or the date of the change. It would appear to the physician that it is the patient who is the source of the data, not a clinician from a previous care visit or encounter. At this point, the physician would treat the data as he or she would any patient sourced data. For this to happen in a trusted manner, the truth of source would have to be preserved such that the consumer would not be able to modify the change in attribution.

These are simply two examples of approaches the standards community has taken to balance privacy with data integrity. AHIMA and HL7 does not represent that these are the system functions that should be used to balance privacy and data integrity. They are merely ones the PHR WG has developed in response to input from consumer advocates and countries outside the US. Clear policy needs to be developed in this area after which standards can be aligned. Until then, these criteria represent consensus-based approaches.

Based on discussions in the HL7 and ISO work groups on EHR requirements, other consensus-based approaches were developed (this list may not be exhaustive). For brevity's sake, we merely list them in a table, but will not discuss them here.

Contact Information

Donald T. Mon, PhD
Vice President, Practice Leadership
American Health Information Management Association (AHIMA)
233 N. Michigan Ave., 21st Floor, Chicago, IL 60601
(312) 233-1135 (Office)
(312) 233-1435 (Fax)
(708) 250-4374 (Cell)
Donald.Mon@ahima.org
www.ahima.org
www.myPHR.com

Table 1
Other Consensus-based Approaches
Identified by the HL7 and ISO Work Groups
Focused on the PHR

The consumer can withhold data by:

- Not entering data into the record in the first place
- Selecting only certain portions of professionally sourced data to import into the record
- Limiting or revoking system access to data to certain individuals (including the physician)
- Masking the data (showing that data is present, but has a mask over it)
- Hiding the data (the data is contained in the record but does not appear to the physician to be present)
- Deleting professionally sourced data with or without audit traceability
- Modifying professionally sourced data with or without audit traceability
- Modifying professionally sourced data with a change in attribution (it's now the patient providing the information, not a clinician from previous care)
- Controlling the export of health information from the PHR (what data is exported and who it is exported to)

Conclusion

PHRs will be viable in the future. There are definite problems in which PHRs can be part of the solution, but it will take time and financial investment. In addition, the issues that we've outlined in this testimony will need to be addressed before PHRs can be a true part of the solution.

References

Grossman JM, Zayas-Cabán T, Kemper N. Information Gap: Can Health Insurer Personal Health RecordsMeet Patients' And Physicians' Needs? *Health Affairs* 28, no. 2 (2009): 377–389; 10.1377/hlthaff.28.2.377

Halamka JD, Mandl KD, Tang, PC. Early Experiences with Personal Health Records. J Am Med Inform Assoc. 2008;15:1–7. DOI 10.1197/jamia.M2562.

Kaelber DC, Shah S, Vincent A, Pan E, Hook JM, Johnston D, Bates DW, Middleton B. The Value of Personal Health Records. Center for Information Technology Leadership. 2008. Charlestown, MA.

Rishel W, Handler TJ. M.D.Patient-Changed Data Is a Threat to PHR Credibility. 23 October 2008, ID Number: G00162311

Simborg D. The Limits of Free Speech: The PHR Problem. J Am Med Inform Assoc. 2009;16:282–283. DOI 10.1197/jamia.M3069.

Tang PC, Ash JS, Bates DW, Overhage JM, Sands DZ. Personal Health Records: Definition, Benefits, and Strategies for Overcoming Barriers to Adoption. J Am Med Inform Assoc 2006 Mar-Apr;13(2):121– 6.

Appendix 1
AHIMA'S PHR Efforts

AHIMA's Previous Experience with PHRs

AHIMA has reached out to consumers in two major ways: first, through a consumer-oriented web site, **www.myPHR.com**, and second, through a series of presentations—from small church groups to hospital-sponsored health fairs to support groups (e.g., prostate cancer, diabetes)—held in communities across the country and led by an AHIMA-trained Community Education Coordinator (CEC). The primary goals of our outreach efforts are:

- To increase public awareness and understanding of the issues surrounding personal health information and health records
- To provide consumers with the information they need to better manage their personal health information and to encourage them to maintain a PHR in order to improve the quality of care they receive

Both myPHR.com and the CEC presentations have been growing steadily. The following activities have occurred to date:

- myPHR.com is the number one returned search result on both Google and Yahoo! when searching "personal health record," and is listed in the top five for "health record." MyPHR.com received a record 850,000 hits in the month of February 2008 and currently averages 135,000 hits per month while the prior year saw monthly averages of 24,000 hits. There has also been a consistent increase in "time spent per visit."

- First and second quarters of 2008 saw the launch of the campaign with the release of the CEC presentation kit DVD, revamped Web site and press releases on the campaign and myPHR.com. A PHR public service announcement was released nationally to 250 television stations representing the four major networks and cable television programs. A radio version was released to 450 radio stations. AHIMA's CEO also conducted a nationwide radio media tour. Hosted by longtime network news anchor Hugh Downs, the six-minute "mini-documentary" was released to public broadcasting and cable news stations as one segment of a 10-part health and wellness series. The documentary was also posted on YouTube.com and Google Video.

- The Nielson Company reported reaching an audience of more than 24 million viewers with its public service announcement. AHIMA's radio media tour with CEO Linda Kloss aired on 23 stations in 10 markets with an audience of almost three million people.

- Media kits have been distributed to more than 2,000 news media outlets. Articles have been published in *Prevention Magazine*, the *Chicago Tribune*, CNN.com, *AARP Magazine,* the *Wall Street Journal*, *USA Today*, *Healthcare IT News, For the Record,* and numerous others.

- More than 150 presentations have been delivered to local communities exceeding our goal for the campaign year. Volunteer support has been incredible with approximately 100 CECs and more than 750 local presenters established. Analysis of the participant evaluations is still ongoing. Survey results will help determine future development and campaign enhancements.

Contact Information

Donald T. Mon, PhD
Vice President, Practice Leadership
American Health Information Management Association (AHIMA)
233 N. Michigan Ave., 21st Floor, Chicago, IL 60601
(312) 233-1135 (Office)
(312) 233-1435 (Fax)
(708) 250-4374 (Cell)
Donald.Mon@ahima.org
www.ahima.org
www.myPHR.com