



AHIMA Comments to ONC on Personal Health Records – December 2010

Note:

The comments below were submitted by AHIMA to the Department of Health and Human Services (HHS) Office of the National Coordinator for Health Information Technology (ONC) in December of 2010. Because these questions and the responses were not part of a formal proposal by ONC, the agency chose to have individuals and organizations respond by answering the questions, one-at-a-time, via an on-line mechanism. There was no formal letter involved.

The Office of the National Coordinator for Health Information Technology is seeking public comments on issues related to personal health records. Please submit comments by visiting one or more of the following questions. Please note that your name and comment will be placed on the public record of this roundtable, including on the publicly accessible HHS/ONC website (links below).

The public comment period will close on December 10, 2010. Thank you for your submission.

[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?

AHIMA believes that PHRs can have significant benefits to individuals to allow for education and information, including research and trials, as well as the ability to hold an informed conversation with providers. PHRs ability to provide individuals the use of their personal information to seek outside references (on-line) holds considerable promise. In addition knowledge and understanding of one's personal health information can lead to improved involvement of individuals in their care.

We must caution that providing information for such searches must be couched in terms that will promote dialogue with the individual's provider and not set providers against such information uses. The capability to seek and receive such information should be available in any form of PHRs so as to allow for more specific search and receipt of information. This would potentially eliminate any translation errors between the individual's diagnosis as provided by the provider and the information sought. Patently to do this, uniform terminologies, classifications, and data definitions must be used.

It has been suggested by some AHIMA members that vendors building new PHR models should look to what consumers are using in non-healthcare sectors, rather than having the industry force models on the public that have been designed without consumer (or provider) input.

We are concerned that there is considerable uncertainty due to the current state of e-health development and the various levels of engagement by individuals in their healthcare. This includes using portals, personal health records (PHR), and the various available models and technologies. It is clear from HITECH that such models must have security protection no matter what model is being used and short of a provider portal (available only to the provider and the authenticated individual/patient) the patient must have control.

At present the healthcare industry has some oversight of organizations offering defined PHR models in the form of HIPAA-HITECH regulations through the HHS Office of Civil Rights or HITECH-FTC. We believe that anyone having access to patient identifiable healthcare associated information should be made liable for any intentional or unintentional misuse of the information which would include the sharing of such information beyond informed patient consent or authorization as required by HIPAA-HITECH and applicable state or federal law. In addition, such patient identifiable healthcare associated information should not be permitted to inappropriately discriminate against an individual. In either case the offending organization or individual should be prosecuted and penalized.

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?

Our collective experience is that there is no common expectation or attitude related to the collection and use of health information in PHRs. We also believe that many PHR vendors do not have a common belief or understanding of their privacy and security obligations related to PHRs. That aside, we also believe that most individuals believe that PHRs are covered by “HIPAA” even if they do not understand just what HIPAA does or does not cover.

The consumer holds onto an expectation that the confidentiality, privacy, and security of their health information will be protected. In addition a good number of consumers believe that laws, regulations, and enforcement authorities already exist.

Bloustein¹ stated that “words we use to identify and describe basic human values are necessarily vague and ill defined.” He regarded individual privacy as, in part, a spiritual issue, the unprivileged invasion of which is an affront to individual privacy and human dignity. Beyond the spiritual and emotional issues that surround patient control over their personal health information the National Committee on Vital and Health Statistics² stressed the lack of clear definition as an

¹ Bloustein,, Privacy as an Aspect of Human Dignity: An Answer to Dean Posser. 39 NYU Law Review, 962, 1001, 1967.

² National Committee on Vital and Health Statistics (NCVHS). (2006, June), A broad review of privacy, confidentiality, and the nationwide health information network. Privacy Report: Recommendations on Privacy and Confidentiality, 2006 – 2008. U.S. Department of Health and Human Services.

issue that often clouds discussions regarding confidentiality, privacy, and security. The myriad of definitions and opinions contributes to the general difficulty differentiating among “privacy,” “confidentiality,” and “security.” As a result these terms are often used interchangeably and imprecisely.

For the purpose of their report the NCVHS adopted the definitions from the Institute of Medicine (2006) report “Disposition of the Air Force Health Study”:

- Privacy is an individual’s right to control the acquisition, uses, or disclosures of individually identifiable health information.
- Confidential refers to the obligations of those who receive information to respect the privacy interests of those to whom the data relate.
- Security refers to administrative, technological, and physical safeguards used to protect individually identifiable health information from unauthorized access, use, or disclosure.

In spite of numerous definitions no single set of uniform definitions of confidentiality, privacy, or security exists. No single industry-wide entity has assumed an absolute leadership role with regard to establishing a standardized set of policies and procedures. In the age of the electronic health record it is odd that no standard patient consent model policy and procedure exists. Individual views regarding privacy and confidentiality differ widely. Personal opinions are influenced by the patient’s health condition, ethical, cultural, religious beliefs, traditions, or practices.

Is there empirical data that allows us reliably to measure any such consumer expectations?

While our AHIMA members are aware of numerous studies by a variety of organizations we know of no empirical data in part because of the variance in personal expectations related to privacy and the multitude of PHR models currently offered.

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?

Expectations vary with the organization being searched and AHIMA and its members have no data beyond anecdotal comments. We are aware that some segments of the population have trust in government-related sites while others do not and are afraid of how their search might come back to haunt them personally. When consumers use their own healthcare providers’ sites (usually portals) there appears to be more confidence in the security of the site (unless the provider or organization has had a publicized breach), but for the most part consumers are not aware of their legal protections, even if clearly stated on the site. An expectation of surveying entities to prominently post a notice that addresses these concerns (similar to the requirement to post a privacy notice) is not an unreasonable requirement and should require the individual to “accept” or “reject” prior to proceeding with completing the survey.

How determinative should consumer expectations be in developing policies about privacy and security?

Consumers have the right to expect privacy and security and to be informed of the organizations policies, procedures, and practices as well as consumers' rights with their respective organization.

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?

Con: Confusion will be heightened for those covered by the rule as well as the consumer! There is considerable overlap in healthcare entities involved with patient information and the rate of change in technologies and social networking add to this overlap and confusion. Security must be maximized, but we know that this is an ongoing effort that is accomplished within organizations' economic constraints. This is why we believe that those persons or entities misusing healthcare data must be the target of prosecution. Different requirements also make it harder for oversight organizations to monitor compliance.

Much of the focus, with regard to privacy and security requirements for non-covered entities, centers around whether PHR vendors and custodians are covered under HIPAA or HITECH. Suitable IT security governance frameworks exist outside of HIPAA and HITECH, yet not much is heard about compliance with these IT security governance frameworks. ISO-17799 an international standard published by the International Organization for Standardization , is the most obvious for information security. The ISO-17799 has a corresponding certification process whereby an entity can become ISO-Certified. In addition the IT Infrastructure Library (ITIL) published by the Office of Government contains security management guidelines based on the ISO-17799 standard. Security standards beyond HIPAA and HITECH are available to PHR vendors and custodians and should be employed.

Con: Any and all PHRs, portals, etc., must be built in such a way that:

- the consumer can understand what is available,
- where the information comes from,
- what are the impacts of decisions that the consumer might be asked to make with this product, and
- the ability to have a source to answer any technical questions including privacy policy and practices as well as security options.

Terms used currently such as "opt in" or "opt out" in reality do not have common meanings. Additionally, privacy and security requirements for PHR vendors should be well drafted in order to address any possible vendor exemption request similar to Google's current stance.

Pro: An expectation of requiring entities to prominently post a notice that addresses these concerns (similar to the requirement to post a privacy notice) is not an unreasonable requirement and should require the individual to "accept" or "reject" prior to proceeding with completing the survey.

Any Other Comments on PHRs and Non-Covered Entities

Do you have other comments or concerns regarding PHRs and other non-covered entities?

As noted, AHIMA believes that personal health information should be protected no matter where it resides and how it is being used. This includes any model of a PHR and current non-covered entities. Further, it is essential that future development and use of PHR technology be done in such a way to ensure equal access