

The Office of the National Coordinator for
Health Information Technology



About the PHR Model Privacy Notice

Background, Development Process, Key Points

September 2011

Overview

In order for individuals to engage in their health and health care, they need information. Under Federal law, individuals have a right to access and obtain a copy of their health information from health care providers and health plans. Some individuals may choose to store and manage their health information using a personal health record (PHR). As more individuals obtain access to their electronic health information and use PHRs to manage this information, it is important for them to be aware of PHR companies' privacy and security policies and data sharing practices.

The PHR Model Privacy Notice ("Model Notice") is a tool that PHR companies can use to communicate their privacy and security policies and data sharing practices to individuals. This novel, Web-based tool provides a uniform and easy-to-understand approach for PHR companies to be transparent about certain key privacy and security issues. By making this Model Notice available, PHR companies can help build greater trust in PHRs and promote competition on policies that are more consumer-protective.

Being better able to compare PHRs will empower individuals to make informed choices. Like the FDA nutrition facts label, the Model Notice is intended to enable companies to present complex information in a manner that is accessible, consistent, and conducive to informed choice. Unlike the FDA nutrition facts label, use of the Model Notice is voluntary.

The Model Notice was developed based on consumer testing that identified key issues individuals care about and language that they understand. Of course, we expect we will learn a great deal from individuals and PHR companies as this Model Notice is put into use, and we look forward to getting feedback and improving it over time.

Background

Information held by an individual in a PHR may not be subject to legal requirements that limit the release of personal information by a PHR company. Therefore, it is important that individuals understand the privacy and security policies and data practices of the PHR company.

Some PHRs are offered by health care providers and health plans covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule. The HIPAA Privacy and Security Rule applies to these PHRs. However, some PHRs are offered by organizations not covered by HIPAA, and, in these cases, it is the privacy and security policies of the PHR company as well as any other applicable laws, which govern how information in the PHR is protected.

In June 2008, the Office of the National Coordinator for Health Information Technology (ONC) began a multi-phase, iterative research project to develop a clear, easy-to-understand, at-a-glance PHR Model Privacy Notice that could be used by any PHR company (whether the PHR is covered by HIPAA or not). The project's goals were twofold: 1) to increase individuals' awareness of PHR companies' data practices; and 2) to empower individuals by providing them with an easy way to compare the data practices of two or more PHR companies.



The Model Notice is a template PHR companies can easily populate with their data practices. The notice's uniformity and simplicity allow individuals to recognize the standardized Notice, quickly learn and understand privacy and security policies and data sharing practice information, compare PHR company practices, and make informed decisions.

Similar to the FDA Nutrition Facts Label and the Schumer Box for credit card disclosures, this approach does not mandate specific policies. Instead, it helps encourage transparency of key product facts that can empower individuals to make informed choices.

Process

ONC contracted with Kleimann Communication Group, Inc. to develop a PHR Model Privacy Notice that would meet the goals state above. This tool was developed in three phases.

- Phase 1 - Understanding the Landscape: This phase included conversations with Federal experts in the area of privacy notices and privacy practices; an in-depth environmental scan and analysis of relevant background materials (such as individual communication literature, actual PHR privacy policies, and other published analyses); and a limited round of individual testing. A draft PHR Model Notice was released by HHS in December 2008.
- Phase 2 - Public Stakeholder Input: This phase included solicitations and review of public comment and input from stakeholders in the public and private sector, individuals, and communication specialists.
- Phase 3 – Consumer Testing and Tool Development: This phase focused on further rounds of in-depth consumer testing to assess and analyze individual understanding of the PHR Model Privacy Notice and further adjust the notice using individual input.

The contractor conducted forty-two formative and cognitive usability tests with consumers during 2009-2010. First, formative tests sought understanding of individuals' awareness and exposure to PHRs, privacy, and data practices. This was the basis for the content foundation and strategy for the PHR Model Privacy Notice design and functionality. Next, the contractor used cognitive usability testing to develop the integrated PHR Model Privacy Notice. This testing helped establish comprehension baselines and design decisions and ultimately to test functional components in an on-line environment. Participants were a mix of age, gender, income, geographic location, education level, race and ethnicity to ensure a wide audience could readily use the PHR Model Privacy Notice. Because PHR users are Internet users by definition, the test subjects were primarily individuals who regularly use the Internet for transactions, such as on-line banking.

Key Points About the PHR Model Privacy Notice

- This PHR Model Privacy Notice focuses on transparency to enable individual choice. It does not establish privacy policies. Much like a “soup can label,” it requires transparency about the practices (or ingredients) but does not specify the practices that must be followed.
- The PHR Model Notice focuses on a PHR vendor’s data practices (i.e., the “back end” data movement of the vendor’s default data practices). The “front end” choices an individual might make about sharing their PHR data for personal health management (for example, a choice to share personal health information in a PHR with a treating physician or caregiver) are not part of the scope of this PHR Model Notice.
- Use of the model notice is voluntary. We hope many PHR companies will value transparency—and recognize that their customers do too—and use this notice to communicate with individuals.
- ONC developed this PHR Model Privacy Notice as a tool. ONC does not enforce use of the tool. However, if a PHR company under the jurisdiction of the Federal Trade Commission (FTC) does not adhere to the privacy and security commitments stated in their PHR Notice, the FTC has authority to challenge the notices as false or misleading in violation of the FTC Act.
- This notice is intended to be used by a PHR company to communicate with individuals. It is not intended to address legal requirements that may apply to a PHR company. We anticipate that PHR companies will continue to make available more in-depth privacy notices.
- We provide on our Web site a template for PHR companies to use to create a notice from the PHR Model Privacy Notice, an implementation guide to help PHR companies fill out and use the Model Notice, and a consumer guide that will provide greater explanation to individuals about the terms and implications of the Model Notice.
- This is Version 1.0. While we based the Model Notice on research aimed at understanding how individuals think about these issues, we are interested in feedback from companies who are the early users of this notice and from individuals who view the notice. We anticipate that we will be able to improve this Model Notice in the future based on such feedback.