CDT Issues Privacy Recommendations for PHRs

by Harley Geiger [1]
July 26, 2010

The Center for Democracy & Technology today released a report [2] recommending privacy and security protections for personal health records (PHRs). CDT believes PHRs should be subject to comprehensive policies comprised of a mix of legal requirements and voluntary best practices. CDT's recommendations – summarized below – are designed to preserve public trust in PHRs and enable the field to flourish.

A PHR is essentially an electronic tool that enables consumers to store, manage, use, and share their personal health information. A key characteristic of PHRs is the high degree of control the individual consumer – not the health care provider – has over the service, including what data gets uploaded to the PHR and with whom it is shared. Through PHRs, people can monitor chronic conditions, explore treatment and insurance options, ensure their health information is correct, share data with others to gain insight and support, and hold their providers to high standards of accountability. However, the success of PHRs will depend in substantial part on whether consumers trust that their sensitive information is protected.

Numerous studies indicate [3] that privacy is a top reason for consumer reluctance to adopt PHRs. This concern is not speculative. Many PHRs are not covered by major privacy and security oversight regulations for health information. For consumers, this means fewer assurances that their information is adequately safeguarded. For industry, ambiguity or inconsistency in regulations can chill innovation and investment that can improve the quality of PHR services. A comprehensive policy framework for PHRs is the most effective means of providing clarity for the marketplace and greater protection for consumers.

Specialized Regulations are Needed for PHRs

HIPAA – the nation's foremost health privacy law – applies only to those PHRs offered by HIPAA-covered entities (such as health providers or payers) or their business associates. However, PHR services are increasingly offered by entities outside the traditional coverage of HIPAA, including search engines, software manufacturers, online health sites, and financial institutions. No single federal statute clearly or adequately applies to these PHRs with regard to consumer privacy protection.

Expanding HIPAA to cover all PHRs is not a good solution. The HIPAA Privacy Rule was created to regulate the sharing of medical information in control of providers, and does not translate well to PHRs designed for consumer control. For example, HIPAA does not require patient consent to disclose personal health information for treatment, payment, and health care operations. Such policies are inconsistent with the concept of PHRs as tools operated at the consumer's direction.

Rather than extending HIPAA, CDT believes that a superior approach would be to construct new regulatory policies adapted specifically to PHRs that draw from HIPAA and other sources. These rules should protect consumers by restricting PHR vendors from engaging in certain practices, or by providing individuals with certain rights that go beyond those currently provided under HIPAA. The regulatory framework should also offer incentives for PHR vendors to engage in best practices based on the Markle Common Framework for Networked Personal Health Information [4].

Custom Policies for Individualized Products

CDT's report – Building a Strong Privacy and Security Policy Framework for PHRs – recommends baseline rules for PHRs and urges the adoption of comprehensive best practices based on the Markle Common Framework. CDT's proposals are primarily directed at Congress and federal regulatory agencies seeking to initiate protections for consumers using PHRs. Among other things, CDT

recommends regulators:

- *Require consumer consent to collect, use and disclose data in a PHR*: The baseline standard for collection, use, and disclosure of personal health information in the PHR should be a clear opt-in consent that is not conditioned on the use of the service. Specific consent should be required for any data collections, uses, or disclosures of personal information that would be unexpected or considered sensitive by a reasonable consumer. However, relying too heavily on notice and consent often places the onus of privacy protection on consumers and confers the bulk of the bargaining power with service providers. CDT therefore urges the regulators to be vigilant of, and take action to prohibit, unfair marketing practices in the PHR space.

- *Establish a safe harbor to encourage best practices*: A safe harbor should not just encourage mere compliance with legal requirements, but rather promote industry best practices that are more comprehensive than what the law requires. Safe harbor strategies grants favorable treatment, such as exemption from certain liabilities or penalties, to actors who meet the safe harbor standards. The requirements should mirror the policy and technology expectations in the Markle Common Framework, which go beyond CDT's proposed PHR regulations. The safe harbor regime must have independent approval and oversight components.

- *Require PHR providers to be transparent about their relationships with third-party applications and websites*: The same federal policies that apply to PHR providers should be extended to their third-party applications and websites. PHR providers also should clearly communicate to users the precise nature of their relationships with these applications and websites. PHR providers should state clearly what privacy and security protections the PHR provider takes responsibility for, and what responsibilities are left to the discretion of the third-party applications and websites.

- *Require PHRs to adopt reasonable security and oversight mechanisms*: PHR providers should adopt reasonable security protections, including technical, administrative and physical safeguards. In particular, PHR providers should adopt strong user authentication policies and immutable audit trails.

- *Prohibit the re-identification of aggregate or de-identified data from a PHR*: PHR rules should include a strong prohibition against unauthorized re-identification of data obtained from PHRs, including penalties for those who inappropriately re-identify. PHR vendors should be required to use rigorous methods to prevent re-identification.

- *Require strong and consistent enforcement of rules*: An effective enforcement scheme for PHRs should, at a minimum, include authorization to both federal and state consumer protection authorities to enforce the provisions, criminal and civil penalties set at a level that provides a strong incentive for compliance with the law, clear audit authority, Regular public reports to Congress by federal regulators on enforcement, and a limited private right of action.

Empowering a Tool for Action

PHRs could help bring about significant changes in health care, providing consumers with an effective way of storing, managing and sharing their health data. But consumers must trust that data they share and store via their PHR is properly safeguarded. Yet federal law presently offers only a patchwork of protections and does not effectively address the concerns of consumers who use these services. CDT calls on regulators to enact rules and incentives for industry best practices that will bring clarity and consumer protection to the PHR marketplace.

- PHR
-
- Markle
- hipaa

- Health Privacy
- health

The content on this website that originates with CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. Details.
Copyright © 2013 by the Center for Democracy & Technology.
Source URL: https://www.cdt.org/blogs/harley-geiger/cdt-issues-privacy-recommendations-phrs

Links:
[1] https://www.cdt.org/personnel/harley-geiger
[2] http://cdt.org/files/pdfs/Building_Strong_Privacy_Security_Policy_Framework_PHRs.pdf
[3] http://www.chcf.org/~/media/Files/PDF/C/ConsumersHealthInfoTechnologyNationalSurve y.pdf
[4] http://www.connectingforhealth.org/phti/