Request for information on the new federal health data breach notification provisions to be administered by the Department of Health and Human Services. [1]

May 21, 2009

Robinsue Frohboese
Acting Director and Principal Deputy Director
Office for Civil Rights
United States Department of Health and Human Services

Dear Ms. Frohboese:

The Markle Foundation's Connecting for Health Initiative has since 2002 brought together leading government, industry, and health care experts to accelerate the development of a health information-sharing environment to improve the quality and cost-effectiveness of health care. The Center for Democracy and Technology (CDT), through its Health Privacy Project, promotes comprehensive privacy and security policies to protect health data as information technology is increasingly used to support the exchange of health information. We submit these comments in response to the request for information issued by the Department of Health and Human Services (HHS).

The thrust and starting point of our comments rest on the need for a consistent and consumer-oriented approach to privacy and security policies for personal health records (PHRs). We understand this issue will be broadly addressed in the forthcoming HHS and FTC privacy and security recommendations for PHRs, but we strongly recommend that HHS and FTC take this early opportunity to align policies and make them meaningful to consumers who must be able to navigate their use of PHRs.

In June 2008, Markle Connecting for Health released the Common Framework for Networked Health Information, [2] outlining consensus privacy and security policies for personal health records and other consumer access services. This framework — which was developed and supported by a diverse and broad group including technology companies, consumer organizations and HIPAA-covered entities[3] — was designed to meet the dual challenges of making personal health information more readily available to consumers, while also protecting it from unfair or harmful practices.

A foundational principle of this work is that a consistent and meaningful set of policies for protecting information in personal health records is desirable for consumers, whether the PHR is offered by a HIPAA-covered entity or not. However, this does not imply that

[1] Federal Register/Vol. 74, No. 79/April 27, 2009
[2] See www.connectingforhealth.org/phti.
[3] See list of endorsers of the Markle Connecting for Health Common Framework for Networked Personal Health Information at the following URL: http://www.connectingforhealth.org/resources/CCEndorser.pdf.

it is appropriate to simply extend HIPAA coverage in its current form to uncovered entities supplying PHRs or new health information products. The approach of the Connecting for Health Common Framework was to develop a set of meaningful policies and practices that are appropriate for all entities that may provide consumers with personal health record services. Another core principle is that personal health records and other consumer access services are tools for consumers' use, and are controlled and managed by consumers. With such services, consumers may keep electronic copies of personal health information and health-related transactions generated through their interactions with health entities, collected by health-monitoring devices, or contributed by themselves.

It is critical that these basic consensus policies be considered in HHS' implementation of the breach notification provisions applicable to HIPAA-covered entities and business associates. It will be confusing and potentially harmful to consumers to have different protections and rules for PHRs depending on the legal status or business model of the offering entity, and even more so if the policies do not consistently support meaningful consumer participation in and control of these emerging and powerful tools.

In summary, we urge HHS to:

- Ensure PHRs will have consistent and consumer-oriented privacy and security protections, including breach notification provisions that are appropriate to personal health records; and
- Support a study of state breach notification provisions to determine whether the new federal provisions conflict with existing state law, or state and federal laws will result in individuals receiving duplicate notices.

Although ARRA requires HHS to issue an interim final rule on breach notification by August 18, 2009, we urge HHS to follow the lead of the FTC and issue proposed breach notification regulations before that date if possible,[4] allowing for more thorough public consideration and comment on these critical issues.

I. Ensure PHRs will have consistent and consumer-oriented privacy and security protections, including breach notification provisions

Personal health records hold significant potential for consumers and patients to become key, informed decision-makers in their own health care. By providing individuals with options for storing and sharing copies of their health records, as well as options for recording, storing, and sharing other information that is relevant to health care but is often absent from official medical records (such as pain thresholds in performing various activities of daily living, details on side effects of medication, and daily nutrition and exercise logs), personal health records can be drivers of needed change in our health care system.

[4] We acknowledge the multiple ARRA implementation issues on HHS' agenda.

In order to feel comfortable using PHRs, consumers need assurance that their information will be collected, used, or disclosed according to their preferences. It is reasonable for consumers to expect they will be able to authorize who may access any data they contribute or authorize to be contributed to any network-accessible PHR, and that they will be able to review audit logs of all disclosures of their records.

As noted above, among the policies endorsed in the Markle Connecting for Health Common Framework for Networked Personal Health Information is that individuals should have the choice of whether or not to open a PHR account, and individuals should choose what entities may access or exchange information into or out of that account.[5] This foundational policy is reflected in the definition of a PHR in ARRA: "an electronic record of information on an individual "that is managed, shared, *and controlled by or primarily for the individual*."[6]

Section 13424(b) of ARRA requires HHS (in consultation with the FTC) to report to Congress no later than February 18, 2010, with recommendations for privacy and security requirements for PHR vendors and related entities that are not covered by HIPAA as either covered entities or business associates. We urge HHS to rely on the Markle Connecting for Health Common Framework in developing its recommendations. It is not desirable to simply extending HIPAA in its current form and entirety to new entities without careful review of the policies and practices that may be appropriate to the specific instance of personal health records.[7] The Common Framework recommendations include policies and practices that are common to all entities, yet may be tailored to meet the specific consumer expectations based on their relationship with the entities they chose to supply PHR services to them.

Although HHS does not have to report its recommendations to Congress until early next year, the breach notification requirements that apply to PHRs will go into effect no later than September 18, 2009. The agency has an immediate opportunity to adopt consistent and consumer-oriented policies, like the Common Framework.

HHS and FTC should adopt consistent information and breach policies for PHR tools that give individuals the ability to input, store and control their own health information. Consumer confusion will result if products that are similarly marketed as having patient control actually have significantly different standards. Consequently, we urge HHS in promulgating its breach notification rule to clarify that, with respect to a PHR offered by a covered entity or a business associate, the breach definition language "unauthorized acquisition, use or disclosure," means acquisition, use or disclosure of protected health information without the authorization of the individual. We posit that this approach is

---

[5] See http://www.connectingforhealth.org/phti/reports/cp3.html.
[6] Id. (emphasis added).
[7] See http://www.cdt.org/healthprivacy/HIPAA-PHRs.pdf for a more detailed explanation of why the HIPAA regulations in their current form are inappropriate for protecting consumers using PHRs.

required to appropriately implement ARRA's definition of a PHR as being an electronic record of information on an individual "that is managed, shared, *and controlled by or primarily for the individual*."[8] It is also consistent with the FTC's proposed breach notification standard.

This standard would apply to products marketed as a means for consumers to control, manage and share their health information, consistent with ARRA's definition of PHR. The tools might hold copies of the consumers' information from the provider's medical record, combined with information input by the consumer or from other sources. However, none of the above suggestion regarding PHRs should suggest any change to the rules governing a covered entity's operational record (e.g., their legal medical record) and its permitted uses of data captured in such operational records of the covered entity. In the operational record context, HHS should interpret the breach definition in Section 13400 of ARRA consistent with those rules.

II. HHS should further study consistency of ARRA breach notification provisions with state laws

HHS should further study consistency of ARRA breach notification provisions with state laws. HHS asks a number of questions in the RFI about possible conflicts between the ARRA breach notification provisions and the breach notification requirements in state laws. At least 44 states, the District of Columbia, Puerto Rico and the U.S. Virgin Islands have data breach notification requirements,[9] and to the best of our knowledge, three states (Arkansas, California and Delaware) have laws that expressly apply to health data. There is insufficient time to review the provisions of these laws to appropriately address HHS' specific questions, and we hope the agency will not draw any specific conclusions or modify its proposed approach to implementing the HIPAA breach notification provisions based on blanket statements about possible conflicts or speculation that individuals might be subject to receiving multiple notices.

However, we recognize the possibility that there could be issues that need to be resolved, and we suggest that HHS work with Congress to call for a study – perhaps by the Government Accountability Office or the Congressional Research Service – to review state breach notification laws and address the questions raised by HHS in the RFI. The agency will then have objective data upon which to base its decisions, or to use to approach Congress if the agency thinks statutory changes are needed.

[8] Id. (emphasis added).
[9] http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm.

III. Conclusion

We appreciate the opportunity to provide these comments in response to HHS' RFI on the ARRA breach notification provisions that apply to HIPAA covered entities and business associates. In summary, we ask HHS to:

- Ensure PHRs will have consistent and consumer-oriented privacy and security protections, so that consumers can have reasonable expectations for policies that will protect their use of such services.
- Support a study of state breach notification provisions to determine whether the new federal provisions conflict with existing state law, or will result in individuals receiving duplicate notices.

Please let us know if you have any questions or need further information.

Sincerely,

Markle Foundation
Center for Democracy & Technology