WORLD **PRIVACY** FORUM

August 2, 2007

Simon P. Cohn, M.D., M.P.H.
Chairman, National Committee on Vital and Health Statistics
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

Re: Response to June 21, 2007 NCVHS letter *Update to privacy laws and regulations required to accommodate NHIN data sharing practices*

Dear Dr. Cohn:

The World Privacy Forum is a non-partisan, non-profit public interest research group. We focus our work on in-depth analysis of privacy issues, including original research. Health care privacy is a core area for the World Privacy Forum.[1] The World Privacy Forum was pleased to have the opportunity to testify on medical identity theft before the NCVHS Privacy and Confidentiality Subcommittee in 2005.[2] Our work on medical identity theft was pioneering and is ongoing.

The Committee's June 21, 2007 letter to the Secretary of Health and Human Services, *Update to privacy laws and regulations required to accommodate NHIN data sharing practices,* has come to our attention.[3] The World Privacy Forum commends the Committee for its work on this subject. The hearings that the Committee held on privacy practices of entities that use health information in their day-to-day operations but that are not covered by HIPAA were timely, informative, and useful. The hearings contributed significantly to general understanding of the scope of the problem and the gaps in the current regulatory approach. So does the Committee's letter.

We particularly note the Committee's observation that the non-covered entities "may even sell personal health information without authorization for the purpose of marketing or other purposes that consumers may find objectionable." The World Privacy Forum agrees with the

[1] See <http://www.worldprivacyforum.org>.
[2] See <http://www.worldprivacyforum.org/testimony/NCVHStestimony_092005.html>.
[3] See <http://www.ncvhs.hhs.gov/070621lt2.pdf>.

Committee, and believes that the use of identifiable patient health care information for marketing is a disturbing possibility. New institutions are being developed and implemented to exploit gaps in HIPAA that allow use of patient data for marketing purposes. Action to close those gaps is needed urgently. The Committee's letter is a small step in that direction.

The World Privacy Forum generally agrees with the Committee's conclusion that *all entities that create, compile, store, transmit, or use personally identifiable health information should be covered by a federal privacy law*. We might be inclined to go a bit further and suggest that all entities that create, compile, store, transmit, or use personally identifiable health information should be covered by *the same* federal privacy law, but the difference here is minor.

We would like to call your attention some HHS activities that fall outside of HIPAA and that the Committee did not mention in its letter. We start from the Committee's analysis of one particular category of non-covered entities:

> In the first category are entities that do not submit claims for payment in electronic form. These entities are not covered because the definition of a covered provider is connected to the original purpose of HIPAA — administrative simplification of the processing of claims. Since these entities do not submit claims or bill health plans electronically, they fall outside the definition and are not covered. Among the health care providers not covered by HIPAA are entities that are directly paid by their customers or another party, such as some of the following providers: cosmetic medicine services, occupational health clinics, fitness clubs, home testing laboratories, massage therapists, nutritional counselors, "alternative" medicine practitioners, and urgent care facilities.

We believe that this analysis is fine as far as it goes. We have two HHS activities to add to your list of significant health care activities that create health records not subject to HIPAA or other privacy rules.

Our first example comes from the Food and Drug Administration's Risk Minimization Action Plans, or RiskMAPs. The relevance of RiskMAPs in the context of the Committee's analysis is illustrated by the patient tracking system established for the acne medication isotretinoin (Accutane and its generics). Patients taking the drug are required to participate in an FDA-approved registry called iPledge. We have no position on the need for patient education or monitoring for this drug. However, we are concerned with the FDA's inattention to privacy in this area, and the resulting privacy consequences of that neglect.

In the iPledge program, for example, detailed patient information is collected and maintained in a database by a third party hired by the pharmaceutical manufacturers. While the disclosure of patient information is a required element of treatment, patient health information ends up in the hands of an entity that is neither a direct health care provider nor a business associate of a provider. The FDA's view is that the iPledge registry is not subject to HIPAA.[4]

[4] We are not sure that the FDA's position is necessarily correct, but this is not the place to argue the point. The effect of the current policy is to leave patient data unprotected by HIPAA, and that is what brings it within the NCVHS discussion of the gaps in HIPAA coverage.

The effect is that there is a large patient registry of approximately 100,000 people whose treatment and other information is not covered by privacy rules. The potential consequences are well-illustrated by the privacy policy of the iPledge registry -- a policy that expressly allows the use of patient data for marketing purposes. That policy may be changing, but it is not because either HIPAA or the FDA requires a different result. The records are simply not regulated for privacy.

We have discussed the policy issues associated with RiskMAPs and the iPledge program in various forums. Our comments are available at <*http://www.worldprivacyforum.org/pdf/WPF_FDAiPledge_08012007fs.pdf*> and at <*http://www.worldprivacyforum.org/pdf/WPF_RiskMAP_FDA28June2007fs.pdf*>. The broader concern here is that similar risk management programs may create pools of unprotected patient data that could be used in ways contrary to the HIPAA privacy rule and contrary to patient expectations. In some ways, this example falls at the more serious end of the spectrum because the majority of patients will not be likely to appreciate that an activity inextricably intertwined with health care treatment falls outside the protections of HIPAA. By contrast, patients are less likely to be confused in this way about health information disclosed to a fitness club.

Our second example comes from an important organization that is not covered by the HIPAA privacy rule. Indeed, we believe the organization to be the largest health care provider in the United States not required to comply with HIPAA privacy and security standards. That organization is the National Institutes of Health (NIH), a part of the Department of Health and Human Services.

The failure of the Secretary to write a health privacy rule that covers NIH is poor policy, and it sets a poor example to the health care system and the Nation. The confluence of circumstances that exempted NIH from coverage under HIPAA are an accidental result of the interplay between a policy decision about NIH patient billing made years ago for other reasons plus the tying of the HIPAA rule's scope to the billing practices of health care providers. The end result gives the appearance that HHS exempted a significant part of itself from a privacy rule that it sought to impose on most of the rest of the health care world.

Not all of the privacy deficiencies that you identified in your letter can be readily cured without major legislative action. However, the Department can and should take immediate action to bring NIH under HIPAA. The necessary change would not take congressional action. The Secretary has the authority to change the HIPAA rules or to take other actions that would make NIH comply with HIPAA. The World Privacy Forum believes that this action is long overdue. Departmental actions can also address the privacy shortcomings of FDA's RiskMAP programs.

We do not know if there are other components of HHS or of other federal agencies that provide health care but which are not HIPAA covered entities. This might be a small but fruitful area of further inquiry by the NCVHS.

We ask that you share this letter with the other members of the Committee. We also invite you to post it on the Committee's website.

Sincerely,

/s/

Pam Dixon
Executive Director
World Privacy Forum