June 21, 2007

Honorable Michael O. Leavitt
Secretary
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

Re: Update to privacy laws and regulations required to accommodate NHIN data sharing practices

Dear Secretary Leavitt:

On June 22, 2006, the National Committee on Vital and Health Statistics (NCVHS) sent you a letter report, *Privacy and Confidentiality in the Nationwide Health Information Network*. Among the 26 recommendations was the following:

R-12. HHS should work with other federal agencies and the Congress to ensure that privacy and confidentiality rules apply to all individuals and entities that create, compile, store, transmit, or use personal health information in any form and in any setting, including employers, insurers, financial institutions, commercial data providers, application service providers, and schools.

The NCVHS held a series of three hearings in 2006-2007 to learn more about the health privacy practices of entities that make significant use of health information in their day-to-day operations but are not covered by the Health Insurance Portability and Accountability Act (HIPAA). At the first two hearings, we heard from representatives of life insurers, insurance regulators, human resource professionals, occupational health physicians, financial institutions, primary and secondary schools, and colleges. The third hearing focused on health care providers and other entities in the health industry that are not covered by the HIPAA privacy rule. We inquired about the degree to which they are regulated by other federal or state laws and the possible effects that federal health privacy coverage would have on their operations.
What we learned from the testimony strongly reinforces our conviction that all entities that deal with personally identifiable health information should be covered by some federal privacy law. The NCVHS would like to share with you some additional observations in support of our earlier recommendation with respect to this last group of non-covered entities, those operating in the health care arena.

A significant concern is that many of the new entities essential to the operation of the Nationwide Health Information Network (NHIN) fall outside HIPAA's statutory definition of "covered entity." Health information exchanges, regional health information organizations, record locator services, community access services, system integrators, medical record banks, and other new entities established to manage health information have proliferated in recent years.

While some of these entities may be business associates under the Privacy Rule, and thus obligated by contractual agreements with covered entities to maintain similar standards, others may not be business associates. Moreover, it is the view of the NCVHS that business associate arrangements are not sufficiently robust to protect the privacy and security of all individually identifiable health information. Business associates are subject only to contract claims brought by the covered entity and not to enforcement actions by HHS or the Department of Justice. The health information technology community is moving quickly in response to the Department's efforts on the NHIN, but our hearings have revealed that, even today, numerous individually identifiable health records are not subject to federal privacy and security protections. This remarkable fact underscores our view that all individually identifiable health information created, collected, stored, or transmitted should enjoy the protections of a federal privacy standard.

In addition to new entities that manage health information, mentioned above, NCVHS also heard from representatives of non-covered healthcare providers: the National Athletic Trainers' Association, the International Medical Spa Association, a large employer participating in a multi-employer personal health record system, a health record bank organization, and a home testing laboratory. We also heard from legal experts who addressed various issues associated with these entities, such as the status of medical practices that operate on a cash only basis and the disposition of the health records of entities that enter into bankruptcy.

Based on the testimony we heard, we now understand that a significant number of everyday providers of health care and health-related services are not covered by the HIPAA privacy and security rules. These entities fall into two categories. 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.

In the second category are providers that create records covered by the Family Educational Rights and Privacy Act (FERPA) which are explicitly excluded from the definition of "protected health information" in the HIPAA Privacy Rule. FERPA, which is overseen by the Department of Education, protects records of students in schools that receive Department of Education funds. Thus, most health records created and maintained by school clinics fall under FERPA rather than HIPAA. However, some schools are not covered by either law. Some providers, such as athletic trainers working in scholastic athletic programs, or college student health services that submit electronic insurance claims, have reported confusion as to whether they are subject to HIPAA or to FERPA. Today, under separate cover, we are also sending a letter addressing this matter.

The HIPAA privacy and security rules were designed to set minimum, uniform protections for identifiable health information across the nation. Providers of health care and related services not subject to HIPAA may also not be subject to any other state or federal privacy law. This means they may be free to engage in a wide range of practices otherwise not permitted under HIPAA. For example, non-covered entities are not required to provide notices to individuals about their privacy practices, train their staffs about privacy and confidentiality, institute physical controls on the storage or use of health records, protect electronic transmissions of health information, maintain an accounting of disclosures, or require an authorization before re-disclosing health information to other non-covered entities. These entities may even sell personal health information without authorization for the purpose of marketing or other purposes that consumers may find objectionable.

In the context of the NHIN, it will be easier to design health information products and services with knowledge of privacy requirements than to retrofit them to new privacy policies. Therefore, time is of the essence.

> **Recommendation:** HHS and the Congress should move expeditiously to establish laws and regulations that will ensure that all entities that create, compile, store, transmit, or use personally identifiable health information are covered by a federal privacy law. This is necessary to assure the public that the NHIN, and all of its components, are deserving of their trust.

We appreciate the opportunity to share with you our findings and recommendation on this important issue.

Sincerely,
/s/
Simon P. Cohn, M.D., M.P.H.
Chairman, National Committee on
Vital and Health Statistics

Cc: HHS Data Council Co-Chairs