Public Health Data Standards Consortium

624 N. Broadway Room 382 Baltimore MD 21205
Phone: 410-614-3463 Fax: 410-614-3097
E-mail: aorlova@jhsph.edu

February 22, 2006

Governor
Address
State

Re: Office of the National Coordinator for Health Information Technology's "Privacy and Security Solutions Project"

Dear Governor,

The ***Public Health Data Standards Consortium*** (The Consortium) is very pleased to express its support of your state's proposal for the Health Information Security and Privacy Collaboration (HISPC) project. HISPC is being implemented by the U.S. Department of Health and Human Service's Office of the National Coordinator for Health Information Technology (ONC) under contract with RTI International and in collaboration with the National Governors Association. The goal of HISPC is to develop a process that will allow states to identify and resolve privacy and security barriers to health information exchange across states and territories to facilitate the development of a national health infrastructure.

To this effect, the Consortium wants to encourage active participation of the public health sector in your state's initiatives on health information privacy and security. Many efforts at standardizing privacy and security have not fully considered the needs of the public health sector in its mission to provide services and protect the health of the public. These services provide the foundations for the larger health care industry, and lack of full participation could lead to significant impairment of the public sector's ability to positively impact the overall health of individuals and communities.

The Consortium is a not-for-profit, voluntary confederation of national, state and local government agencies, professional associations, and public and private sector organizations established to represent the interests of the public health community in the national standards development process and bring a common voice from the public health community to these efforts. The Consortium's main goals are to educate and empower the public health sector, facilitate consensus among the public health players, and bring public health sector concerns to national attention. The Consortium's involvement goes beyond data standards alone to include health system interoperability; privacy and security; electronic health records; common public health vocabularies; and prioritizing and communicating key public health sector needs in each of these efforts.

Public health brings a unique perspective to discussions of privacy and security. While public health agencies and organizations are often not perceived as part of the health care industry, they indeed have contributed to successfully preventing, controlling and eradicating diseases, such as poliomyelitis and small pox. Clean water and air, monitoring and regulating hazardous materials, investigating and controlling infectious disease, and providing education and preventive care are all public health activities that have improved the general health of people and communities worldwide. This population-based perspective creates different approaches to care and prevention, and requires using and exchanging health information in different ways.

Public health has a long history of balancing individual privacy rights with protecting and improving the overall health of the general population, and has long had strong privacy protections for the health information it collects, maintains, uses and exchanges. Public health often works with the most sensitive types of health information, such as on HIV/AIDS, on reproductive health, and on chronic diseases and behavioral health, where strong protections are necessary to provide public assurance of confidentiality. There are two main concerns for public health in the privacy and security discussion: first, that health information protections may be so stringent that health care entities will limit or refuse to share information for public health purposes; and second, that the strong historical public health privacy protections may be eroded in the national effort to attain uniformity to support interoperability and affect the public's confidence and willingness to share patient's health related information that is needed to formulate and implement public health programs aimed to improve the health conditions of individuals and communities in our country.

The Consortium has provided the following list of common public health concerns on privacy and security to assist in your state's efforts:

- Public health activities such as biosurveillance, disease tracking, contact tracing and disease reporting are critical in protecting and improving the health of the population. Public health entities must be able to conduct these activities rapidly and thoroughly as any impediments to timeliness can mean additional lives affected. However, public health uses of health information are also highly dependent on the public trust. Privacy and security protections must be crafted to enable and facilitate these essential public health functions while preserving to the greatest extent possible the privacy of individuals.

- Public health activities such as biosurveillance, disease tracking, contact tracing and disease reporting currently suffer from the persistent failure of health care providers to report complete and accurate data or to report at all. This failure is often the result of labor-intensive manual processes and a multiplicity of reporting forms, requirements, and systems. More complete information will aid public health to better understand causes of disease conditions and improved response effectiveness. Promoting a health information infrastructure that removes this multiple data entry burden would facilitate better public health response and reduce reporting error. Privacy and security protections should be crafted to remove policy and regulatory barriers to reporting and consider adding incentives for compliance.

- Public health is generally not perceived as an equal partner by the private sector, or sometimes it is considered as just a minor player, in the health care industry. Privacy and security barriers are therefore often unjustifiably used as excuses for not sharing information with public health agencies, as these are perceived as a burden and not related to the business of health care. Privacy and security protections should be crafted to recognize the needs of all health care participants in the larger continuum of health and health care for the individual and the population, and strive to balance all participant needs to render timely and effective protection, response, and care.

- Privacy and security are often used as a rationale for preventing comprehensive data integration to allow public health to take the next step to practice "whole-person" disease surveillance and intervention activities. Only with the "whole-person" approach can the association between disease and risk behaviors or exposures or means of transmission be seen. Privacy and security protections should allow for using patient's health related information in new ways and in new combinations within appropriate parameters to allow forward movement in understanding and improving overall health while preserving to the greatest extent possible the privacy of individuals.

- Public health activities and responses are increasingly becoming globalized and facilitated by regional, national, and worldwide electronic systems and networks. Privacy and security protections must take into consideration the need to work with and across national boundaries, systems and laws to support global surveillance and response while protecting confidentiality and applying appropriate security measures.

- In a world of routine international travel and commerce, new and existing infectious diseases such as SARS and bird flu can travel quickly and be difficult to control. Instant communication mechanisms are increasingly vital for worldwide public health efforts in identifying and controlling potential pandemic situations. Privacy and security protections must eliminate barriers that allow public health authorities to respond immediately to any potential public health threat.

- The movement to electronic health records must take into consideration the need for notification and easy public health access to records as needed to provide the necessary information for conducting public health activities. Privacy and security protections must be crafted to enable and facilitate public health access with minimal barriers while preserving to the greatest extent the patient's privacy.

- Current concerns with bioterrorism or highly communicable diseases require a real-time link between public health on the front line and public health entities at local, state and federal level. For example, an isolated case of anthrax might not be perceived as an act of terrorism, but reporting cases from more than one location may point to a more orchestrated and calculated threat. By linking the isolated incidents epidemiologic and public health practices can be applied and appropriate responses mounted. Privacy and security issues related to patient's health related information reporting, storing and sharing is a critical need for public health practice and must be considered in a national health information technology infrastructure.

The Consortium is also prepared to work with your state and your office in the coming months in any other manner that may assist you in this important effort. Specifically, the Consortium will be pleased to provide expertise and additional input from the public health perspective, and assist your state in evaluating the findings and recommendations for public health fit. The Consortium is also available to discuss other avenues of participation that states may find of value as they begin to implement this important project.

The Consortium endorses your state's plan and would be happy to assist you on the national privacy and security process in any way that may be beneficial to your state.

Sincerely,

Walter G. Suarez, MD, MPH
President

Anna Orlova, Ph.D.
Executive Director

Vicki Hohner

Vicki Hohner, MBA
Co-Chair
PHDSC Privacy, Security, and Data Sharing Committee

R C Urbano

Richard Urbano, Ph.D.
Co-Chair
PHDSC Privacy, Security, and Data Sharing Committee

cc:
David Brailer, MD, Office of the National Coordinator for Health Information Technology
Susan Christensen, J.D., Agency for Healthcare Research and Quality
John Thomasian, National Governors Association
Charles R. Thompson, Ph.D., Vice President, RTI International