NACCHO
National Association of County & City Health Officials
The National Connection for Local Public Health

09-06

STATEMENT OF POLICY
Health Information Technology Privacy and Security

Policy

The National Association of County and City Health Officials (NACCHO) recognizes the need for the secure use and exchange of health information for public health purposes. Data standards and regulations should allow for a secure highly defensible interoperable exchange of information such as clinical settings, governmental public health agencies, and academic and research institutions through a secure health information exchange network.[1]

NACCHO also supports the efforts of national health information technology (HIT) stakeholders to develop appropriate privacy and security standards and policies that sustain and improve local health departments' (LHDs) capacity to exchange information securely and to participate in research and policy development.

NACCHO recommends the following:

> Federal and state laws that address health information and privacy should be harmonized and updated to recognize the reality of health information technology. They should also accommodate existing legal mandates that allow for LHDs to have access to identifiable health information, for example through the provisions in the Health Insurance Portability and Accountability Act (HIPAA) regulations. The proposed 2010 HIPAA update announced in July would strengthen the privacy of health information and to help all Americans understand their rights and the resources available to safeguard their personal health data.[2]HHS is working to ensure that as they expand the use of health information technology to drive improvements in the quality and effectiveness of our nation's health care system, Americans can trust that their health information is protected and secure.[3]

- LHDs should participate in the development of state and national initiatives to standardize privacy and security policies, principles, procedures, and protections for information access for population health purposes.[4]

- The Department of Health and Human Services and other relevant federal agencies should provide financial support to do the following:
    - Facilitate LHD participation in the development of resources and educational opportunities, particularly those focusing on standards, health information exchange (HIE) integration, research, and requirements associated with LHD accreditation; and
    - Enable LHDs to utilize the resources and education opportunities that are developed.

- All stakeholders should adhere to the principles outlined in the Office of the National Coordinator for Health Information Technology's (ONC) *Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information*.[5]

- Privacy rules should support the use of HIT in carrying out essential public health functions, such as conducting public health surveillance and producing public health intelligence, and should prevent impediments to public health emergency responses.

Justification

The need for health information exchange is compelling. Public health requires clinical data to improve detection of public health emergencies and adverse events and to improve the overall health of the community. Clinical operations can use data from ancillary services and public health to improve quality of care. There is a need, however, to balance privacy and security concerns with the ability of governmental public health entities to exchange health information with clinical partners. Without further efforts at a federal, state, and regional level, there is a risk that an optimal balance will not be achieved.

According to a 2007 Health Information Security and Privacy Collaboration (HISPC) report, *Privacy and Security Solutions for Interoperable Health Information Exchange*, the mix of HIPAA rules, other federal laws that protect sensitive data, and state-based privacy laws, produces complicated circumstances where the requirements are not always clear.[6] Moreover, according to the State Alliance for e-Health, many state privacy and security requirements are old as they were created for paper-based systems. Most of these requirements also have a low level of consistency as a result of being spread across various state laws and regulations.[7] This poses a unique challenge for LHDs when carrying out their role of surveillance and reporting information that is vital to the development and maintenance of HIEs.[8]

The HISPC report also recommends that states work to harmonize with federal laws that impose additional requirements, such as patient permission for disclosure, on the exchange of certain types of health care information. Examples of such requirements are the Family Education Rights and Privacy Act and the Clinical Laboratory Improvement Amendments. It is important to clarify terms in federal legislation to ensure that there are no unnecessary barriers to the expansion of public health surveillance and community health assessment to capture chronic disease or environmental health data in order to mitigate and prevent health risks, while at the same time promoting the protection of the individual. At the core of being able to exchange information is getting people to allow their information to be captured. Unless systems are put in place that are proactive in their intrusion detection and monitoring, with policies for responses to these threats, confidence of the individual will remain low.

Efforts at the federal, state, regional, and local level to exchange electronic health information between public health entities and healthcare providers for purposes of establishing a National Health Information Network (NHIN) are currently underway. The U.S. Department of Health and Human Services has identified the need to work with public health stakeholders and consumers to effectively harmonize privacy and security mandates across states so that personal health information is "protected and electronically exchanged in a manner that respects variations in individuals' views on privacy and access," while upholding the ability of public health entities to carry out their core functions and respond to public health emergencies.[9]

Part of that standardization process has already begun with ONC developing the *Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information*. The principles set out in the framework lay the foundation for common dialogue.

LHDs must work proactively to encourage and support the adoption of harmonized privacy and security polices within the states and through collaborative national efforts, in particular on those concerning certification. Furthermore, they must be supported by relevant federal and state agencies to engage at this level.

Without adopting these measures, the interoperable exchange of information between public health and clinical systems through the NHIN will be impossible to achieve and the nation's health will suffer as a result.

Record of Action
Approved by NACCHO Board of Directors
July 2009
Updated June 2012

---

[1]Such stakeholders may include the Department of Health and Human Services (DHHS), the Office of the National Coordinator for Health Information Technology (ONC), the Health Information Security and Privacy Collaboration (HISPC), and the Healthcare Information Technology Standards Panel (HITSP)

[2] Department of Health and Human Services Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act. July 14, 2010. Accessed June 2, 2012 at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/nprmhitech.pdf

[3] Department of Health and Human Services Strengthens Health Information Privacy and Security Through New Rules. July 8, 2010. Accessed June 2, 2012 at http://www.hhs.gov/news/press/2010pres/07/20100708c.html

[4] National initiatives include the National eHealth Collaborative (NeHC, formerly AHIC Successor, Inc), ONC's HIT Policy Committee, the Certification Commission for Healthcare Information Technology (CCHIT), and the Public Health Data Standards Consortium (PHDSC).

[5] ONC. Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information. December 15, 2008. Accessed February 6, 2009 at http://www.hhs.gov/healthit/privacy/framework.html

[6] HISPC. Privacy and Security Solutions for Interoperable Health Information Exchange Assessment of Variation and Analysis of Solutions. June 30, 2007. Accessed on December 18, 2008 at http://www.rti.org/pubs/avas.pdf

[7] State Alliance for e-Health First Annual Report. Accelerating Progress

[8] Using Health Information Technology and Electronic Health Information Exchange to Improve Care. Accessed on June 5, 2012 at http://www.nga.org/files/live/sites/NGA/files/pdf/0809EHEALTHREPORT.PDF

[9] Stoto, MA. Public health surveillance in the 21st century: achieving population health goals while protecting individuals' privacy and confidentiality. Georgetown Law Journal 2008; 96: 703-719.