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

09-06

STATEMENT OF POLICY

Health Information Technology

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' 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 local health departments to have access to identifiable health information, for example through the provisions in the Health Insurance Portability and Accountability Act (HIPAA) regulations. In 2013, the Department of Health and Human Services (HHS) announced the final omnibus rule, which was an update of original HIPAA regulations. These regulations enhanced standards to improve privacy protections and security safeguards for consumer health data. These updates provide the public with increased protection and control over their personal health data. This update was made to ensure HIPAA will protect patients' privacy as health information becomes digitized.[2]
- Local health departments 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.[3]
- The Department of Health and Human Services and other relevant federal agencies should provide financial support to do the following:
    - Facilitate local health department participation in the development of resources and educational opportunities, particularly those focusing on standards, health information exchange (HIE) integration, research, and requirements associated with local health department accreditation; and
    - Enable local health departments to utilize the resources and education opportunities that are developed.

    - Allow federal grant funds to be used to enable local health departments to comply with federal health privacy policies.
- 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*.[4]
- Relevant federal agencies should develop a comprehensive policy to regulate mobile health privacy and security, to ensure consumer privacy protection and to encourage the use of mobile health technologies.
- 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.[5] 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.[6] This poses a unique challenge for local health departments when carrying out their role of surveillance and reporting information that is vital to the development and maintenance of HIEs.[7]

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. HHS 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.[8]

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.

Mobile health describes "the use of portable electronic devices with software applications to provide health services and manage patient information[9] " NACCHO has developed a Statement of Policy that encourages the development and use of mobile technologies by local health departments, as internet-based technologies offer new opportunities to local health departments to communicate with their target populations.[10] However, mHealth is affected by a patchwork of policies related to licensure, privacy and security protection, and malpractice liability.

Currently, HIPAA is the primary legal guideline for mHealth privacy and security. However, HIPAA leaves many questions in regards to mHealth. Transmissions from a medical device may be stored and shared to third party advertisers by device manufacturer or application creator. Data acquired this way could finance an application in this manner. Patients are also not considered covered entities or business associates under HIPAA, offers them no protection when information is collected and transmitted by mHealth applications. Because the law currently leaves mHealth user's information unprotected, it increases the risk of their data being accessed without their consent. Without improved privacy protections, the members of the communities that local health departments serve may be less willing to use mHealth technology, severely limiting the potential outcomes associated with their use. [11] [12]While federal regulators, such as the Food and Drug Administration, have taken the first steps in creating guidelines for mobile health technologies[13], no federal agency truly regulates mobile health privacy and security.

Local health departments 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.

References

[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] "New Rule Protects Patient Privacy, Secures Health Information." *U.S. Department of Health of Human Services*. N.p., 17 Jan. 2013. Web. 10 June 2014.

[3]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).

4 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

[5] 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

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

7 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

[8] 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.

[9] Källander, Karin, James K. Tibenderana, Onome J. Akpogheneta, Daniel L. Strachan, Zelee Hill, Augustinus H A Ten Asbroek, Lesong Conteh, Betty R. Kirkwood, and Sylvia R. Meek. "Mobile Health (mHealth) Approaches and Lessons for Increased Performance and Retention of Community Health Workers in Low- and Middle-Income Countries: A Review." Journal of Medical Internet Research 15.1 (2013): n. pag. National Center for Biotechnology Information. U.S. National Library of Medicine, 25 Jan. 2013.

[10] National Association of County and City Health Officials (2013) Statement of Policy: Use of Internet-based Tools and Mobile Technologies by Local Health Departments. Retrieved Jun. 1, 2014, from http://naccho.org/advocacy/positions/upload/13-01Use-of-Internet-based-Tools-and-Mobile-Technologies-by-Local-Health-Departments.pdf

[11] Y. Tony Yang and Ross D. Silverman, Health Affairs, 33, no.2 (2014):222-227, Mobile Health Applications: The Patchwork Of Legal And Liability Issues Suggests Strategies To Improve Oversight

[12] Joseph L. Hall and Deven McGraw, Health Affairs, 33, no.2 (2014):216-221, For Telehealth To Succeed, Privacy And Security Risks Must Be Identified And Addressed

[13] Content of Premarket Submissions for Management of Cybersecurity in Medical Devices." U.S. Food and Drug Administration (n.d.): n. pag. 14 June 2013. Jun. 1, 2014.

Record of Action

Approved by NACCHO Board of Directors July 2009
Updated June 2012
Updated July 2014