

Statement by James I. Golden, PhD,
State Government HIT Coordinator
and
Director, Division of Health Policy
Minnesota Department of Health

Before the
U.S. Department of Health and Human Services
HIT Policy Committee
A Federal Advisory Committee

September 18, 2009

U.S. Department of Health and Human Services
HIT Policy Committee
A Federal Advisory Committee

Statement of James I. Golden, PhD, State Government HIT Coordinator, Minnesota Department of Health

September 18, 2009

Good morning Vice-Chairman Dr Paul Tang, Dr Blumenthal and committee members. Thank you for holding this meeting and allowing me the opportunity to participate on the use, disclosure, secondary uses, and data stewardship panel and how it specifically relates to population health and public health.

The Minnesota e-Health Initiative is a private-public collaborative whose vision is to accelerate the adoption and use of health information technology in order to improve health care quality, increase patient safety, reduce health care costs and improve public health. It is guided by a legislatively chartered, statewide advisory committee with 25 representatives from broad stakeholder groups affected by and interested in electronic health records and other health information technology (HIT).

The Minnesota Legislature charged the Minnesota Department of Health with leading this initiative since its inception in 2004. The work of our e-Health Initiative has resulted in several achievements including the development of a statewide plan providing a framework for the Minnesota health care community to meet state mandates for adoption of electronic health records and help providers become meaningful users. In addition, the e-Health Initiative published four guides relating to adoption of HIT and the effective use of electronic health records. In all of our efforts, population health and public health have been considered and included in our efforts.

Acknowledgements

The success of the Minnesota e-Health initiative over the past five years is due in large part to the leadership and contributions of the Minnesota e-Health Advisory Committee members. The committee is co-chaired by Dr. Jennifer Lundblad CEO of Stratis Health and Walt Cooney, Executive Director of the Neighborhood Health Care Network. In addition several workgroups are and have been convened and thousands of hours of volunteer time are and have been committed to collaboratively examine and resolve issues related to health information exchange and further advance health information technology (HIT) progress in Minnesota.

Population and Public Health Defined

In Minnesota, the following definitions are used for Minnesota-e-Health related activity.

Population Health (everyone's responsibility)

Population health is an approach to health that aims to improve the health of an entire population. One major step in achieving this aim is to reduce health inequities among population groups. Population health seeks to step beyond the individual-level focus of mainstream medicine and public health by addressing a broad range of factors that impact health on a



population level. An important theme in population health is importance of social determinants of health and the relatively minor impact that medicine and healthcare have on improving health overall.

Public Health (governmental responsibility)

Public health is concerned with threats to the overall health of a community based on population health analysis. Governmental public health agencies provide the backbone to the public health infrastructure, but this infrastructure is also dependent on other entities such as the health care delivery system, the public health and health sciences academia, and other sectors that are heavily engaged and more clearly identified with health activities

Public Health Responsibility

Governmental Public Health is a legislative directive; a responsibility to protect, maintain and improve the health of all people in Minnesota. It carries out this responsibility while maintaining the integrity and confidentiality of the information entrusted to it. Maintaining the privacy and security of public health information is critical to upholding the core values of public health including:

- **Integrity**
We are honest, trustworthy and transparent in all we do. We strive to do the right thing to achieve the best public health outcomes.
- **Collaboration**
We value diversity and the unique contributions of our employees and partners. We develop positive relationships, foster innovative solutions, and strengthen our capacity to accomplish our mission.
- **Respect**
We uphold a standard of conduct that recognizes and values the contributions of all. We foster a working environment in which listening to and understanding our differences is encouraged and confidences are protected.
- **Science**
We use the best scientific data and methods available to guide our policies and actions to promote healthy living in Minnesota. We rely on the objective facts of evidence-based science to build a strong foundation to address health needs and concerns.
- **Accountability**
We are effective and efficient managers of the public trust and funds, and hold ourselves and others to appropriate high standards. We interoperate with open communication, transparency, timeliness, and continuous quality improvement.

Public Health Privacy

The Minnesota e-Health Initiative understands that patient privacy protections are paramount both in private and public health settings. Strong security protections, uniformly implemented, regardless of health care setting are essential to successfully protect the privacy and confidentiality of protected health information.

Public health has a long history of implementing authorized and appropriate security measures to protect the privacy of information collected for public health purposes, identifying and responding to health threats, and improving the health of populations. The Minnesota e-Health Initiative will continue to facilitate dialogue on the most appropriate ways balance the goals of interoperability and exchange to improve care with appropriate privacy and security protections that safeguard individuals' confidentiality.

Public Health Practice

Public health practice often requires the acquisition, use, and exchange of Individually Identified Health Information (IIHI) to perform essential public health activities (e.g., public health and disease surveillance, program evaluation, terrorism preparedness, outbreak investigations, direct health services, and public health research). Such information enables public health authorities to implement mandated activities (e.g., identifying, monitoring, and responding to death, disease, and disability among populations) and accomplish public health objectives. Public health authorities have a long history of respecting the confidentiality of IIHI, and the majority of states as well as the Federal government have laws that govern the use of, and serve to protect, identifiable information collected by public health authorities.

Information technology has rapidly transformed the practice of public health. The tragedy of 2001 drove demand for real-time data to monitor population health and highlights the information management needs of public health. Since then, sophisticated systems have been created to read thousands of pieces of chief complaint text coming from hospital emergency rooms to alert public health staff to unusual syndrome presentations – all in real time, by geography and by age group. This is essential to be able to focus public health efforts to identify and manage specific syndromes efficiently and with the least effect on the overall population. In addition, many communicable disease web-based reporting systems not only serve to monitor population health, they are also capable of sifting through disease reports and producing alerts of a potential reportable communicable disease outbreak. The ability to capture this information and identify potential threats sooner than human eyes can scan and absorb hundreds of reports can potentially save lives and public and private funds. Other public health information technology initiatives that link to clinical practice and which have many potential benefits, include:

1. **Electronic laboratory reporting** - Reporting across state lines from public and private laboratories to local and state public health agencies with planned bidirectional messaging to improve detection and clinical and community disease control.
2. **Immunization registries** - Incorporating decision support into EHRs to automatically letting health care providers know about needed vaccinations and issuing reminder letters.
3. **Web-based electronic birth and death registry systems** - Providing the basis for timely public health monitoring systems, as well as, conveying information more quickly to the Centers for Disease Prevention and Control and the Social Security Administration.
4. **Women, Infant and Children (WIC) programs** - Modeling on-line benefit transfer systems using Smart Cards to efficiently link recipients, local and state WIC programs and vendors.

Public Health and Health Information Exchange

Health Information Exchanges (HIEs) present a tremendous opportunity for public health to develop and promote sound policies and programs to reduce chronic disease rates. Quality of care measurements in chronic disease at the population level foster the knowledge and the ability to improve care and serve as benchmarks for progress. The technology and informatics expertise, particularly in communicable disease and bio-surveillance, can be used as a springboard for public health efforts in prevention of chronic diseases and reduction of adverse maternal and child health outcomes. In particular, the exchange of patient specific information on chronic diseases between the public health and health care sectors is a partnership that could be used to enhance primary prevention – actually keep people from developing chronic disease through community prevention efforts. These efforts should fully utilize the scientific evidence that should come from projects funded by the stimulus package that are meant to reduce chronic disease rates.

We believe that population health status measures represent the other half of the return on the investment equation. It is not sufficient to merely seek improvements in better care for individuals. Rather, we must also keep our eye on overall health status changes to know that the reforms you put in place have their desired impact. The population health improvement goals that are the responsibility of every city, county, state and federal health agency can be better achieved by making public health an active partner in the e-health agenda. In particular, on-going e-health activities should consider the on-going resources and efforts needed to integrate the health care delivery system and public health, such as:

1. Make public health a central partner to the expanding e-health initiatives by ensuring that funding to hospitals and providers have a requirement that reportable disease data are sent electronically to public health agencies. Correspondingly, local public health agencies need increased capital and technical expertise to implement systems that can receive and process these electronic disease reports.
2. Invest resources to facilitate public health agencies working directly with the vendors and providers receiving HIT stimulus funding to assure that the software solutions implemented also work with, and are connected to, public health reporting systems (e.g., immunization registries). Investing resources on the public health side will assure that interoperability and data harmonization is more fully accomplished.
3. Ensure that public health leaders are active partners in the national standards setting and HIT certification bodies.
4. Include public health's needs in HIT workforce development efforts.

We should not be attempting to prevent disease, both infectious and chronic, in the 21st century, using mid-20th century methods. A comprehensive reformed health system in America needs to control costs, expand access, and improve the quality of care. But it also needs to begin focusing on well-being. All four of these crucial mandates will need full integration with a 21st century public health system and the ARRA HIT/HIE initiatives offer the opportunity to be successful in our shared goal of a healthier America.

Considerations / Recommendations for Action

1. Detailed frameworks for protecting the privacy of health information privacy public health related purposes have been extensively discussed in State Legislatures and enacted into law. These discussions have occurred to varying degrees in all states and reflect the often complex and competing needs and desires of different stakeholders.
2. During the course of developing public health policies related to the privacy of health information many stakeholders have participated including consumers to develop and implement deliberate public policies that ensure that the information is securely protected.
3. While in some cases a federal solution may be appropriate and meet many of the identified needs of stakeholders, for public health, States need to continue to have a lead role in public health policy development. Public health activities are based in communities, and states are more closely connected to the local community level and able to reflect the values and desires of the stakeholders. Additionally, States have Federal and state mandates to provide public health services and are best positioned to identify issues, gaps and solutions in meeting those mandates that represent stakeholder values.
4. Current public health frameworks are not uniform or simple. Meaning that applying uniform standards and requirements across systems would be challenging and difficult. Public health systems are complex and varied because they are reflect communities' needs and interests.

The development of the national framework for NHIN should develop capacity that will include several key steps:

1. Recognize the critical role of public health to protect the community and the complex and detailed vetting that has already occurred in each state over many years.
2. Recognize that the privacy and security framework for a particular public health responsibility has been created to address stakeholders' perceptions of the public health threat, the needs and abilities of stakeholders to participate in controlling their information, and the need to balance public health goals with other important public policy priorities.
3. Recognize that some public health responsibilities require individually identified data to protect the public health and improve the health of populations.
4. Identify the key situations or responsibilities where variation among local and states systems occur and incorporate options to address identified variations in the systems as they are further developed.

All privacy and security frameworks have common elements and characteristics. Any information system needs to be robust enough to accommodate all of the characteristics and the local variation in how these characteristics are applied. Examples of these elements and characteristics include:

- **The ability of an individual to participate in the decision to collect, use, or disclose identifiable data.**
 - This element may include the ability of an individual to consent to provide their information, to opt-out after their information has been provided, or to require the inclusion of individuals' information.
 - This element may include a requirement that an individual be provided specific information about any legal obligation to provide information, the intended uses of the information, the ability to further disclose or use the information, the benefits and risks of supplying the information, and the consequences of not supplying the information.
 - This element may include the ability of an individual to limit or restrict either certain data uses or disclosures.
- **The ability of an individual to know how or when their identifiable information has been used or disclosed.**
 - This element may require auditing functions that allow individuals to inquire about any uses or disclosures of their information. Information systems need to be able to document the auditing information necessary to respond to these types of queries.
 - This element may require notifications in the event information is inappropriately used or disclosed.
- **The ability of an individual to access and amend their individually identifiable information.**
 - This element may include the ability of an individual to access their information to more accurately and precisely understand the information.
 - This element may include a mechanism to challenge the accuracy or amend the information to correct inaccurate information.
- **The ability of an individual to challenge compliance with legal privacy and security frameworks.**
 - In some situations, an individual may be able to challenge that an entity is adequately complying with privacy and security requirements. It may be necessary to develop policy and mechanisms to accept and resolve these challenges.
- **The need to maintain role-based access to the data.**
 - Frequently different stakeholders have different rights to access, use or disclose information. Systems need to be able to enforce these role-based interactions with the information.
- **The need to time-limit the use or disclosure of the data.**
 - Individuals' privacy is often protected by limiting the time frame in which data may be used or disclosed. Information systems need to be able to document and enforce these restrictions.

Conclusion

Public health and population health are an integral component of the comprehensive vision for e-health in Minnesota. We believe that including population health and public health in our e-health framework is essential to achieve “effective use” of health information technologies and public health should be included at an achievable level in the initial definition of “meaningful use”. How public health’s needs are included in the concept of meaningful use should increase over time as systems are modernized and the capacity for exchange increases.

The transition of public health from paper systems and stand alone electronic systems to a fully integrate, electronic system capable of exchanging seamlessly with others in the health care delivery system is integral to the success of the HITECH Act and overall health reforms. As we make this transition, it is critical to remember that public health’s current privacy and security frameworks are based on rich dialogues with stakeholders representing many points of view. The privacy and security framework for public health’s participation in a National Health Information Network must build upon and enhance the existing privacy protections.