EXECUTIVE SUMMARY

Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

MARCH 31, 2009

Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

Prepared For:

Pennsylvania Health Care Providers and Policy Makers

By:

The Pennsylvania eHealth Initiative and its Local Health Information Exchange Special Interest Group and Policy Committee

Edited By:

Executive Editor - Glen F. Marshall

Contributing Editor - Bob Mitchell

TABLE OF CONTENTS

EXECUTIVE SUMMARY

For a hospital, clinic, physician practice, nursing facility, or home-health organization considering whether to join a Health Information Exchange (HIE), one of the most important questions is “How does the HIE assure patient privacy and how will it help my organization do the same?” This white paper provides practical guidance to help you find the answer to that question and others like:

- Does the HIE provide a document that spells out the responsibilities of the HIE and of HIE participants?
- How does the HIE host assure that access to health data is limited to individuals who are authorized according to common privacy and security policies?
- How do organizations that contribute information to the HIE assure that they collect, store and communicate legally valid consumer consents for disclosure appropriately?
- How does the HIE host organization, data contributors, and data consumers transmit and store health information securely?
- What safeguards would ensure that only the minimum data necessary is accessed when the HIE use or access patient information for any reason beyond patient care?
- How do HIE hosts, data contributors, and data consumers use common interoperable security technology to assure confidentiality, integrity, authenticity, and accountability?
- How do HIE hosts protect and secure health information from possible theft or loss?

> We are all health care consumers. Each of us has an opinion on the value of health care privacy. Often this opinion is influenced by our own health condition (and whether we feel that our health condition has stigma associated with it). While patients universally want the best health care possible, most are unwilling to abrogate their rights to privacy. So, at its core, the issue is that each of us in good faith has a difference of opinion regarding what is appropriate privacy. The challenge is to design HIEs and clinical information systems to meet the public’s reasonable privacy expectations, while still delivering health information as necessary for effective and efficient health care. *– John P. Houston, vice president, Privacy and Information Security & Assistant Counsel, University of Pittsburgh Medical Center*

Recommendations

This white paper supports recommendations stated in PAeHI’s white paper ***Building a Sustainable Model for Health Information Exchange in Pennsylvania*** (February 22, 2008). The concepts indicated by italicized text are especially furthered by:

1. Design a mechanism for payers to support HIEs through a per transaction / usage fee model should be collaboratively designed with payer organizations and the state.

2. Empower a neutral organization with statewide collaborative capability to bring the diverse array of potential providers and consumers of HIE services to the table to *establish common standards for HIE-related value-added services*.

3. Commission research to assess the feasibility of public utility or public authority models to help finance HIEs which *meet minimum 'core' and/or value-added service standards*.

4. Realign provider payments over the long run to appropriately reward and *encourage use of HIE data* to avoid complications of chronic illness, and eliminate unnecessary, ineffective, or redundant care.

5. *Establish 'core' standards related to HIE implementation* using the same collaborative mechanism as described in #2 above for value-added services.

6. *Accelerate access to pharmacy-related data sources by HIEs* to promote accurate medication reconciliation.

7. Develop a mechanism by which a *single standard consolidated data set* would satisfy all provider-related State data reporting requirements; submission to one State agency and distributed by that agency to other departments or agencies as appropriate.

8. We further recommend that the State's approach to these and other areas of policy be consistent with the guiding principles laid out in ***Connecting Pennsylvanians for Better Health: Recommendations from the Pennsylvania eHealth Initiative*** (April 25, 2007), namely that:

   - Patients come first.
   - *Consumer privacy, security and confidentiality are paramount*.
   - *Multi-stakeholder collaboration* is essential.

PAeHI recommends the robust patient privacy and security protections outlined in this paper, with priority given to the adoption of a common consent form governing patient data disclosure statewide. Collectively, these protections will help build and sustain the desired level of trust among patients, providers, Health Plans, and other stakeholders while balancing those protections with the necessity of adequate, accurate and timely patient data-sharing at the point of care.

> If you try to put together a network of hospitals and practices, nursing homes and home health, if they can't all trust that all of the different members of that network will use that information and protect the information appropriately, they won't participate. That's another level at which it's critically important that the system is designed in a way that is provably secure. The information is secure so that all of those different groups are willing to participate. – *James M. Walker, MD, FACP, chief health information officer, Geisinger Health System*