Ensuring Privacy and Security of Health Information Exchange in Pennsylvania

The Pennsylvania eHealth Initiative *in collaboration with the Pennsylvania eHealth Partnership Authority*

The Pennsylvania eHealth Initiative (PAeHI) |2475 Lindle Road, Harrisburg, PA 17111| admin@paehi.org

EXECUTIVE SUMMARY

Ensuring Privacy and Security – What is new for 2014?

Patients are unlikely to share sensitive health information unless they are confident that their provider will honor their confidentiality. Similarly, health care entities are unlikely to join a health information exchange if they are not confident that their medical records will be kept safe and that the data will be flowing securely.

A key factor in achieving a high level of trust and compliance among individuals, health care providers, and other health care organizations participating in a health information exchange is the development of, and adherence to, a consistent and coordinated approach to privacy and security. Clear, understandable and uniform principles are a first step in developing this approach to privacy and security while building trust, which are all essential to the realization of the considerable benefits of HIE.

It can be a challenge to adopt clear and uniform privacy and security principles in a legal landscape that seems inconsistent and restrictive. Absorbing those principles into a sustainable business model that hits all its required regulatory marks requires strong leadership and the will to get it done to both support the business goals and serve the patients and consumers of Pennsylvania.

In 2012, the Commonwealth established the Pennsylvania eHealth Partnership Authority as the governance entity for HIE in the state. The Authority is moving forward with all the mandates contained in its founding legislation to provide uniform standards and agreements that are produced in concert with stakeholders, along with freely distributed consumer outreach tools and a state consent registry.

PAeHI sees this as the first vital step in Pennsylvania achieving a truly interoperable health information exchange network that both supports and expands the market for such services. The broad topic discussions and outlines contained in this white paper are presented as a tool to spur further thinking about the appropriate methods to interface with the legal requirements as to electronic health information privacy and security, the specific requirements within Pennsylvania, and the workplace challenges of technical and administrative implementation.

KEY DOCUMENTS

Data Use and Reciprocal Support Agreement(DURSA)
http://healthewayinc.org/images/Content/Documents/Onboarding-Artifacts/2011-05-dursa-policy-assumptions-summary.pdf

Business Associate Agreements (BAA)
http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hippahealth-insurance-portability-accountability-act.page

LANDSCAPE AND ROADMAP

The health care industry has had many spirited discussions regarding privacy and security from both the provider and patient perspectives since HIPAA was enacted in 1996. The issues surrounding privacy and security continue to challenge all stakeholders regardless of technological sophistication, particularly those involved in the direct delivery of care. This tension between privacy and security requires collaborative solutions that fairly balance the competing interests between security implemented from a business perspective and with an eye to the bottom line, and the privacy rights and expectations of individuals as to their medical information. Below are some of the highlights presented in this white paper.

Concepts for Information Assurance

Confidentiality | Integrity | Availability

KEY DEFINITIONS

Privacy

(1) The right to have all records and information pertaining to health care treated as confidential. (2) Freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue, unauthorized, or illegal gathering and use of data about that individual. (HIMSS, 2006)

Security

The means to control access and protect information from accidental or intentional disclosure to unauthorized persons and from alteration, destruction, or loss. (HIMSS, 2006) The concepts of confidentiality, integrity, authenticity, and accountability are included in security.

Omnibus Final Rules

The Omnibus final rule clarifications were released in January 2013 to provide additional rulemaking around the HIPAA Privacy and Security Rules. The Omnibus rule was based on statutory changes under the HITECH Act and the Genetic Information Nondiscrimination Act of 2008 (GINA).

Pennsylvania eHealth Information Technology Act

This Act, also known as Act 121 of 2012, established the Pennsylvania eHealth Partnership Authority (Authority) as an independent agency of the Commonwealth and the governance body for the statewide technological health information exchange network it was to build.

PURPOSE

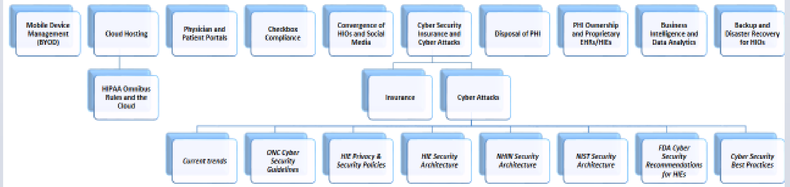
The Pennsylvania eHealth Initiative (PAeHI) is a not-for-profit founded in 2005 by the state's leading health care organizations to transform health care by fostering the broader adoption of electronic health records and health information exchange.

In the sharing of patient data, PAeHI recognizes that robust patient privacy and security protections are essential to build and maintain a necessary level of trust among patients, health care providers, health plans, and other stakeholders. PAeHI also believes that a balance must be maintained between the protection of patient privacy and the adequate and timely sharing of patient data at the point of care.

This white paper addresses health care data privacy and security for electronic information exchange. The key purpose is to help health care providers achieve acceptable data privacy and security assurance for health care consumers, while minimizing cost and confusion. It does not discuss the much broader issues of non-electronic health care data privacy or general security technology.

The regulatory and marketplace landscape has been evolving in a dramatic fashion since the first edition of this white paper in 2009. In order to set that stage, the legal and regulatory sections have been made more in depth to serve as a tool for the provider community. Pennsylvania has also established an independent Commonwealth agency that has been tasked with governing the state health information exchange network of services, establishing and maintaining a common consent registry for patients to opt-out of the exchange, and promoting interoperability within the state HIE marketplace. Much of the updated material in this white paper is reflective of that effort, and is offered here as guidance to the health care community at large.

Emerging Areas of Risk and New Compliance Challenges



For more information about the Pennsylvania eHealth Partnership Authority
http://www.paehealth.org/

CONTRIBUTORS

PA eHealth Initiative
- Robert Torres, Esq.
- Steven J. Fox, Esq.
- William "Buddy" Gillespie
- Dr. Chris Cavanaugh

PA eHealth Partnership Authority
- Alix Goss
- Rebecca Roberts

And special thanks to the PAeHI Committees (BHOX and Policy)

To download a copy -- www.paehi.org