

Protecting Patient Data: Security Compliance Standards for Health Information Exchanges

Good Afternoon Director and members of the Committee. Thank you for allowing Deloitte¹ this opportunity to provide testimony on ways to better protect patient data and instill confidence on the use of the exchange. I am going to discuss patient data protection and assuring security compliance to for Health Information Exchanges (HIEs). Needless to say, building patient trust is a "table stake" to realizing the full potential of HIEs. You asked the following three questions related to security compliance standards which are included in my testimony:

1. To build trust by protecting patient data, what restrictions should there be on permitted uses of data by HIEs?

We believe that building trust comes from a consistent track record; all that it takes is one breach, even of a small scale, to impact trust. There are a few elements to building and maintaining that trust:

- Implement a broad security and privacy risk management program, including a structured risk assessment, to identify threats and countermeasures for the use of data; doing a risk assessment periodically and publishing the high level results helps in building trust.
- Provide easy and secure information to patients about their privacy rights and how their information can and will be used through the use of technology tools such as identity and access management (IAM). IAM is the set of business processes, information, and technology for managing and using digital identities
- Information should be made available on a "need to know" basis and using roles to provide access with robust audit trail capabilities
- Consent management is a system or set of policies for allowing patients to determine who they allow viewing access to their health information. In the absence of a single state consent policy, exchanges will need accommodate multiple consent models
- Adopt clear privacy procedures and train employees so that they understand the privacy procedures and designate an individual to be responsible for determining that the privacy procedures are adopted and followed

The Federal Department of Health and Human Services (HHS) has established a breach notification process with the intent of elevating the citizen trust through regulations requiring mandatory notification procedures. As part of the security program, implement policy, process, technology

¹ As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Protecting Patient Data: Security Compliance Standards for Health Information Exchanges

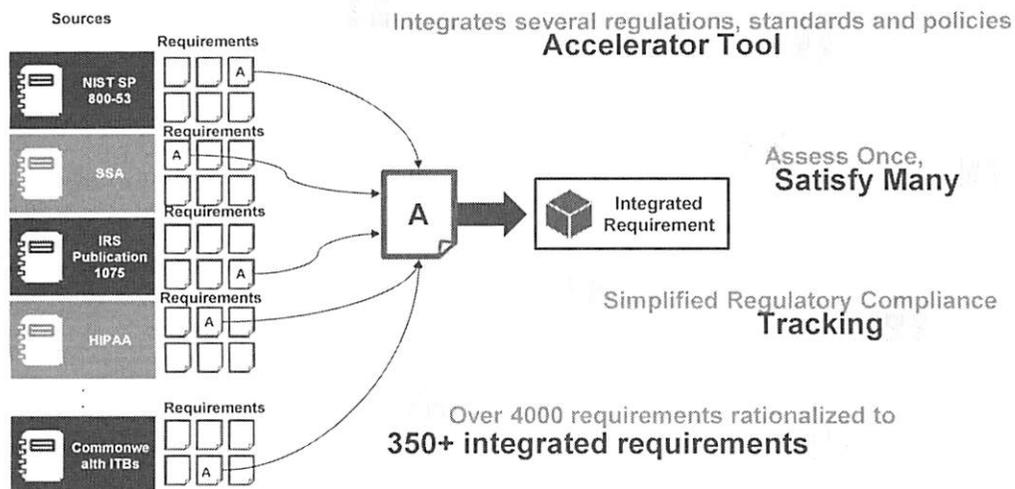
and people changes in the organization to create the cyber awareness and compliance with the mandatory requirements.

2. Which entity or entities should establish and impose security compliance standards on HIEs?

The Office of Health Information and Technology should provide overall governance in establishing and enforcing the security compliance standards on HIEs. OHIT directs the State's HIE implementation efforts and is the custodian for developing a state-level HIE which includes representation from hospitals and universities, businesses, Federally Qualified Health Centers (FQHCs), physicians, nursing homes, insurers, advocates, pharmacies, rural health providers, legislators, the City of Chicago Public Health department, state agencies and the Governor's Office.

One possible approach for establishing security compliance standards and providing a mechanism for continuous monitoring involves using an integrated security regulatory risk framework that rationalizes industry standards, policies, and state and federal laws or regulations. The security risk framework will enable OHIT to assess and prioritize security, privacy and compliance risks, then identify the appropriate risk response strategy, such as mitigating risk through appropriate controls, risk transfer and accepting risk.

The security risk framework can be used to conduct periodic risk assessments on IT assets and processes, select treatment options, monitor the effectiveness of mitigation techniques, and support annual reporting for Federal and State compliance requirements. Figure 1 below illustrates an approach to develop the risk framework.



Protecting Patient Data: Security Compliance Standards for Health Information Exchanges

The integrated security regulatory risk framework rationalization of individual requirements from more than 160 industry regulations and standards and can incorporate applicable security policies, and state and federal regulations. The security risk framework will help enable the State to assess and prioritize security, privacy and compliance risks, then help identify the appropriate risk response strategy, such as mitigating risk through appropriate controls, risk transfer and accepting risk.

3. Should Illinois Health Information Exchange (ILHIE) impose such standards on sub-State HIEs?

ILHIE should collaborate with sub-State HIEs to enforce the standards by providing them the necessary tools and processes to do so.

The security program of ILHIE should include sub-state HIEs. Given that the overall exchange and patient data is only as secure as the weakest link in the complex HIEs, we believe that ILHIE may consider not only providing guidance, standards and tools, but also helping to monitor compliance of these sub-HIEs. Utilizing the security risk framework described above could be once such approach.

By providing an online portal using tools for example by EMC's Archer Governance, Risk and Compliance and/or IBM OpenPages may allow ILHIE too:

- Transform traditional document/paper based audit process to an enterprise system
- Maintain the library of rationalized security and privacy requirements and standards
- Centralize authoritative repository to retain and access audit information
- Facilitate continuous risk, remediation monitoring and report assessment results

In closing, I would like to sincerely thank the committee for allowing me to present today on this important topic related to protecting patient data and look forward for future discussions related to securing HIEs.

Vik Bansal - PMP, CISSP, CIPP, CRISC
Deloitte & Touche LLP
111 South Wacker Drive, Chicago, IL 60606

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation