

Illinois Health Information Exchange Authority
Data Privacy & Security Committee Hearing
July 17, 2012
Chicago, IL

Testimony of:
Lisa A. Gallagher, BSEE, CISM, CPHIMS
HIMSS Senior Director, Privacy and Security
lgallagher@himss.org
Washington, DC

The following prepared testimony is submitted by HIMSS to the Illinois Health Information Exchange Authority Data Privacy & Security Committee for its hearing on privacy and security for HIEs on July 17, 2012 – **Panel #1 - Patient Choice: Options and Permitted Uses for Patient Data.**

About HIMSS

HIMSS is a cause-based, not-for-profit organization exclusively focused on providing global leadership for the optimal use of information technology (IT) and management systems for the betterment of healthcare. HIMSS frames and leads healthcare practices and public policy through its content expertise, professional development, research initiatives, and media vehicles designed to promote information and management systems' contributions to improving the quality, safety, access, and cost-effectiveness of patient care.

HIMSS leads and participates in many HIE/ privacy and security activities as well as providing tools and resources to the healthcare industry through our [HIE Toolkit](#) and [Privacy and Security Toolkits](#).

HIMSS participates at the national level in policy discussions through its participation in activities such as those discussed in the **appendix** to this document.

Background

In connection with the development and implementation of the ILHIE, the Authority is currently developing privacy and security policies relating to the patient data that will be exchanged by the ILHIE. Specifically, the Authority has charged the ILHIE Data Security and Privacy Committee with developing recommendations for possible privacy, security, and consent management policies that may govern the ILHIE.

For Panel 1: Patient Choice: Options and Permitted Uses for Patient Data, ILHIE recognizes that there are different options for patients expressing their preferences regarding the disclosure and use of their electronic health data.

- What patient consent policies should be applied to the operations of the State-level ILHIE?
- Should patients be given a choice whether their electronic patient data is transmitted through an HIE?
- Should they be given a choice with regard to the use and exchange of this data by clinical treatment professionals and others?

- If patients are provided with a choice, should all patients be provided with an option to affirmatively decline (opt-out) or the option to affirmatively consent (opt-in) for exchange of their data through an HIE?

National Level Policy Recommendations

For today's hearing, HIMSS would like to provide a summary of relevant, recent health IT policy recommendations currently being promulgated through law, regulation, guidance and/or recommendations as it relates to the involvement of patients in HIEs. In as much as it is widely recognized that there are differing privacy and security laws that potentially make the interstate exchange of health information challenging and therefore poses potential barriers to HIE implementation, HIMSS feels that state-level HIE activities *can be informed by* federal policy work in this area. (That is, by no means is this information or input from HIMSS meant to be prescriptive or mandatory, but merely informative.) They can also be informed by the activities in other states, but that is not covered in this testimony.

In 2008, ONC developed the *Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information*.¹ The principles in the Nationwide Framework have roots in the Fair Information Practices, or FIPs.² The principles most related to patient choice are excerpted below:

- **Openness and Transparency** – There should be openness and transparency about policies, procedures, and technologies that directly affect individuals and/or their individually identifiable health information.
- **Individual choice** – Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their individually identifiable health information.

The ONC Policy Committee³'s Privacy and Security Tiger Team⁴ has made recommendations related to openness and transparency:

Relevant core values:

- Patients should not be surprised to learn what happens to their health information.
- The provider-patient relationship is the foundation for trust in health information exchange
- Transparency about information exchange practices is a necessary component of establishing credibility with patients.

¹ "The Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information". Office of the National Coordinator, December 15, 2008.

http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__privacy__security_framework/1173

² The most commonly recognized set of FIPs is the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (website): http://www.oecd.org/document/18/0,3746,en_2649_34223_1815186_1_1_1_1,00.html.

³ The ONC Policy committee is a Federal Advisory Committee (FACA) to the Department of Health and Human Service (HHS). See HHS FACA website:

http://healthit.hhs.gov/portal/server.pt?open=512&objID=1149&parentname=CommunityPage&parentid=10&mode=2&in_hi_userid=10741&cached=true

⁴ The Privacy and Security Tiger Team is a workgroup of the ONC Policy Committee. See:

<http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&objID=2833&PageID=19421>

Relevant recommendations:

- Providers are responsible for being open and transparent with their patients about how their data is exchanged.
- Providers should provide a layered notice.

The Tiger Team recently had the opportunity to consider issues of patient consent and choice in its review and response to a Request for Information (RFI) from ONC related to a proposed governance framework for the Nationwide Health Information Network (NWHIN)⁵.

As noted in the NWHIN RFI, consent is meaningful when it:

- Allows the individual advanced knowledge/time to make a decision;
- Is not compelled, or is not used for discriminatory purposes;
- Provides full transparency and education;
- Is commensurate with the circumstances; and
- Must be consistent with reasonable patient expectations for privacy, health, and safety; and must be revocable.

The following is excerpted and paraphrased from the Tiger Team's observations/recommendations⁶:

- Consistency in approach—opt-in or opt-out—is not as important as meeting these specific criteria, which could also be used for validation purposes. <HIE participants should> apply consent with respect to the data sharing it performs or facilitates; consequently, some variation in policy among <HIE participants> is acceptable (and may be necessary in order to accommodate different community norms).
- The Tiger Team agrees that consent (beyond what might already be required by law) should not be required when <an entity> is facilitating secure, directed exchange. However, when the decision regarding whether or not to share health information is no longer in control of the provider, the patient should have meaningful consent about whether or not his/her information is collected, used, or disclosed.
- The Tiger Team has not yet considered whether individual consent should be required for other electronic exchange purposes, beyond what the HIPAA Privacy Rule currently requires.
- The Tiger Team has observed that the relationship between the patient and his or her health care provider is the foundation for trust in health information exchange, particularly with respect to protecting the confidentiality of personal health information. For this reason, the Tiger Team believes that providers should, in most cases, have some responsibility for discussing choice with the patient. Nevertheless, <HIE participants> should also play a role in educating the community

⁵ Nationwide Health Information Network: Conditions for Trusted Exchange, A Proposed Rule by the Health and Human Services Department, 05/15/2012, Request For Information <https://www.federalregister.gov/articles/2012/05/15/2012-11775/nationwide-health-information-network-conditions-for-trusted-exchange>

⁶ The HIT Policy Committee comments regarding the Office of the National Coordinator's (ONC) Nationwide Health Information Network: Conditions for Trusted Exchange Request for Information (RFI): http://healthit.hhs.gov/portal/server.pt/document/958120/application_vnd_openxmlformats-officedocument_wordprocessingml_document

about <HIE participant organization>, its purposes, and its practices, and give providers resources to help educate their patients so that meaningful choice is possible.

Additional Information:

HIMSS would also like to offer the following references as potential resources for the ILHIE Data Privacy & Security Committee as it considers these issues:

- Markle Common Framework⁷, in particular, the Connecting Consumers Common Framework for Networked Personal Health Information,⁸ which describes a comprehensive approach (and tools) for secure, authorized, and private health information sharing.
- Center for Democracy & Technology, “Rethinking the Role of Consent in Protecting Health Information Privacy,”⁹ which “advocates for a new generation of privacy protections that allow personal health information to flow among health care entities for treatment, payment, and certain core administrative tasks *without first requiring patient consent*, as long as there is a comprehensive framework of rules that governs access to and disclosure of health data. Patient consent is one important element of this framework, but relying on consent would do little to protect privacy. This paper also suggests how a framework of protections can provide patients with more meaningful opportunities to make informed choices about sharing their personal health information online.”¹⁰
- Integrating the Healthcare Enterprise (IHE)¹¹ is a standards profiling organization that includes the participation of healthcare professionals and industry to improve the way computer systems in healthcare share information. Systems that support IHE “Integration Profiles” work together better, are easier to implement, and help care providers use information more effectively. The goal is efficient delivery of optimal patient care. Within IHE, specific Integration Profiles that support privacy and security include, but are not limited to, the following:
 - Audit Trail and Node Authentication (ATNA) provides basic security through (a) functional access controls, (b) defined security audit logging and (c) secure network communications.
 - Basic Patient Privacy Consents (BPPC) provides a method for recording a patient’s privacy consent acknowledgement to be used for enforcing basic privacy appropriate to the use.
 - Consistent Time (CT) enables system clocks and time stamps of computers in a network to be synchronized (median error less than 1 second).
 - Cross-Enterprise User Assertion (XUA) communicates claims about the identity of an authenticated principal (user, application, system...) across enterprise boundaries - Federated Identity.
 - Enterprise User Authentication (EUA) enables single sign-on inside an enterprise by facilitating one name per user for participating devices and software.
 - Document Encryption (DEN) encrypts individual documents and portable media content.

⁷ Markle Foundation, Common Framework, <http://www.markle.org/health/markle-common-framework>

⁸ Markle Foundation, Connecting Consumers Common Framework for Networked Personal Health Information (2008), <http://www.markle.org/health/markle-common-framework/connecting-consumers>

⁹ Center for Democracy & Technology, “Rethinking the Role of Consent in Protecting Health Information Privacy,” <https://www.cdt.org/files/pdfs/20090126Consent.pdf>

¹⁰ Ibid.

¹¹ http://wiki.ihe.net/index.php?title=Main_Page

- [Document-based Referral Request](#) (DDR) supports referral requests that are transferred by document sharing (e.g., XDS, XDR, XDM).
- [Document Digital Signature](#) (DSG) is a content profile that specifies digital signatures for documents.
- **HIMSS State HIT Dashboard** is a free HIMSS resource that gives healthcare professionals, policy makers and industry leaders an interactive snapshot of major health information technology initiatives, such as health IT legislation, academic health IT programs, Davies Award winners, Regional Extension Centers and Health Information Exchange organizations. (<http://www.himss.org/statedashboard/>)
- **HIMSS White Paper: “States Will Transform Healthcare through Health IT and HIE Organizations.”** In this report, the HIMSS State Advisory Roundtable looks at state health IT legislation, state initiatives, and challenges faced by states in the implementation of health IT, and provides recommendations going forward. (http://www.linkedin.com/redirect?url=http%3A%2F%2Fwww%2Ehimss%2Eorg%2Fpolicy%2Fd%2F20120605StatesWillTransformHealthcare%2Epdf%3Fsrc%3Dsm&urlhash= fu7& t=tracking_anet)

HIMSS is pleased to be able to provide input to this hearing is available for further discussion. Please contact Lisa Gallagher, lgallagher@himss.org.

Appendix: HIMSS Information

HHS ONC FACAs:

- Standards Committee – Privacy and Security Workgroup (Lisa Gallagher)
- Standards Committee - Clinical Operations Workgroup (Joyce Sensmeier)

Integrating the Healthcare Enterprise (IHE)¹² (Joyce Sensmeier, James St. Clair)

IHE accelerates the adoption of EHRs by improving the exchange of information among healthcare systems. Its goal is to improve the quality, efficiency and safety of clinical care by making relevant health information conveniently accessible to patients and authorized care providers.

Carefully implemented interoperability standards are the foundation of EHRs, PHRs (personal health records) and health information exchanges being established around the world. IHE has developed a foundational set of profiles for secure exchange of patient information across enterprises. IHE profiles support health information networks in Canada and the U.S.A, as well as several Asian and European countries, and have been accepted as requirements by the U.S. Secretary of Health and Human Services for federal procurement of healthcare IT systems.

Joyce Sensmeier (HIMSS) is the current president of IHE USA and HIMSS is a founding organization.

To learn more about HIMSS and to find out how to join us and our members in advancing HIT, please visit our website at www.himss.org.

¹² Integrating the Healthcare Enterprise (IHE) at: <http://www.ihe.org>