Comments of the World Privacy Forum, the Center for Digital Democracy, and Privacy Activism to CalOHII regarding Proposed HIE Regulations Pursuant to AB278

Via email

Azadeh Mohandessi-Fares
CalOHII
1600 9th Street, Room 460
MS 20-10
Sacramento, CA 95814

April 1, 2011

The World Privacy Forum, the Center for Digital Democracy, and Privacy Activism are pleased to offer our comments on the CalOHII proposed regulations published at http://www.ohi.ca.gov/calohi/LinkClick.aspx?fileticket=HIHuxsjVSPc%3d&tabid=36. We understand that as part of AB278, CalOHII is authorized to adopt regulations for demonstration Health Information Exchange projects in California to ensure all participants follow consistent rules.

We are pleased to see the California proposed regulations regarding HIE, and we generally support them. The World Privacy Forum has been deeply involved in the CalPSAB process, serving as co-chair and a consumer representative for Californians in the HIE process for the past two years. The WPF is a non-profit public interest research and consumer education group focused on privacy issues, including health care privacy.[1] The Center for Digital Democracy is a leading U.S. digital privacy non-profit organization that educates the public about the role of consumer data collection used for interactive advertising, especially in the field of online health information and services.[2] Privacy Activism is a California non-profit organization whose goal is to enable people to make well-informed decisions about the importance of privacy on both a personal and societal level. PA has long expertise in the area of medical privacy, and has served on California and national HIE and e-health-related committees.

I. Patient Trust is Crucial to any HIE System in California: Keep Opt-in Consent

Patient trust is at the core of any healthy health information exchange. Without bedrock patient trust in the system, the system will not be used as it was intended, and the cost savings and medical improvements sought by implementing an HIE will not be realized. One of the most important things that the California regulations need to accomplish is to

[1] See http://www.worldprivacyforum.org/.

[2] See http://www.democraticmedia.org/.

encourage patient and even provider trust in the California HIE projects. Transparency, opt-in patient consent, a consent revocation process, and consistent application of Fair Information Practices will be key to the state in earning patient trust.

Information technology has made it easier to collect, collate, analyze, aggregate, and exchange enormous amounts of health information electronically to the benefit of patients and health care providers. But without patient trust, no system will be able to overcome the "doubt factor" despite bells and whistles technologies, and the benefits that could accrue to patients could be lost.

As CalOHII is aware, President Obama followed up on the HIE efforts begun in the Bush administration by authorizing $36 billion in Federal stimulus funds to facilitate the development, testing, and adoption of a spectrum of healthcare information technology tools. These funds include support for critical state-level healthcare information exchange projects and further the development of the National Health Information Network.

Whereas up until now many of the projects related to HIE have not used "live" patient data, now these projects are advancing to use actual patient data in real-world settings.

Rigorous, national, and long-running studies to analyze the requirements for HIE have been consistently undertaken by the US Department of Health and Human Services AHRQ and ONC. These studies, The Health Information Security and Privacy Collaboration,[3] involved the work of 42 participating states and thousands of stakeholders from the health care provider and patient communities. The HISPC studies consistently show that patient trust in the electronic health care exchanges is a core and vital component in adoption of the systems, and that without it, health information exchange programs may suffer from a lack of patient and even provider adoption.[4]

Health information exchange will create much more patient data in electronic formats than ever before in history. Patients are concerned about increased sharing of their health information, even if that sharing is for their benefit. A California HealthCare Foundation study found that 15 percent of patients who know their information will be shared would hide information from their doctor, and another 33 percent would consider hiding information.[5]

---

[3] *Health Information Security and Privacy Collaboration*, RTI International. This DHHS project had as its goal to develop and test solutions for the privacy and security of national and state health information exchange. The series of multi-year studies and reports are available at http://healthit.ahrq.gov/portal/server.pt/community/ahrq_national_resource_center_for_health_it/650 and at http://www.rti.org/page.cfm?objectid=09E8D494-C491-42FC-BA13EAD1217245C0.

[4] Dimitropoulos, Linda. *Privacy and Security Solutions for Interoperable Health Information Exchange: Impact Analysis.* December 2007. Available at http://www.rti.org/pubs/phase2_impactanaly.pdf. See pages 4-7; 4-40.

[5] California Healthcare Foundation, Consumers and Health Information Technology: A National Survey, April 2010. Available at http://www.chcf.org.

This emphasis on patient trust is not new in the scholarly literature, nor is it solely tethered to the adoption of health information technology. The literature is replete with articles describing the importance and influence of patient trust in seeking health care and in maintaining the therapeutic relationship in non-technology related contexts. Without patient trust in various health care settings and situations, research has consistently shown that to varying degrees, patients may not utilize health services.[6]

Given the wealth of data about patient trust in electronic contexts and general health care contexts, it is unsurprising that HHS has continued to insist on the core value of engendering patient trust in health information technology and exchanges. The Department's National Coordinator for Health Information Technology stated in 2010 that:

> "As the Department of Health and Human Services (HHS or The Department) continues its efforts to improve the health and care of all Americans by promoting the advancement of health information technology (IT), one of the Department's guiding principles is that the benefits of health IT can only be fully realized if patients and providers are confident that electronic health information is kept private and secure."[7]

The key buttresses of patient trust are seen by HHS as the expansion of HIPAA's privacy and security protections under ARRA, in particular the provisions that curtail the sale and marketing uses of patient data. Congress recognized in ARRA that patient trust was crucial to the adoption of health information technology, and that without it, systems may be built, but patients may not be willing to seek services if there were questions of inappropriate circulation of patient data.

In order for patients and providers to trust information to flow freely into and through health information exchanges, robust choice for patients needs to exist; this requirement should not be subject to a waiver or any other loopholes.[8] Generally, the proposed

---

[6] See Blumenthal, D (1996). Effects of market reforms on doctors and their patients. Health Affairs, 15(2), 170-184. *See also* Dugan, Elizabeth et al. Development of abbreviated measures to assess patient trust in a physician, a health insurer, and the medical profession. BMC Health Serv Res. 2005; 5: 64. Published online 2005 October 3. doi: 10.1186/1472-6963-5-64. PMCID: PMC1262715. *See also* Chen, Huey Jen (2004). Trust and Health Service Use. Florida Agency for Health Care Administration. Available at http://home.fmhi.usf.edu/common/file/ahca/ahca2004/2004-Chen.pdf.

[7] Statement of Blumenthal, David and Verdugo, Georgina. Building Trust in Health Inforamtion Exchange, Statement on Privacy and Security. US Department of Health and Human Services.July 8, 2010. Available at http://healthit.hhs.gov/portal/server.pt?CommunityID=2994&spaceID=11&parentname=CommunityEditor&control=SetCommunity&parentid=9&in_hi_userid=11673&PageID=0&space=CommunityPage.

[8] Consumer Consent Options for Electronic Health Information Exchange: Policy Considerations and Analysis, Office of the National Coordinator for Health IT, March, 2010. p 2. "The goal of

regulations do a balanced job of ensuring patient consent. As technology progresses, we think it is going to be important to offer a more finely tuned set of consent mechanisms that offer opt-in and out under varying circumstances and for various aspects of the health record, such as sensitive information. The current regulations allow for opt-in consent. **We want to very specifically support opt-in patient consent in the proposed regulations as a critical component to patient trust.**

II. Create a single registry of HIE projects in California and post them publicly

It is crucial that California have a transparent HIE ecosystem that all Californians can readily understand and easily and quickly access. There should be no secret HIE projects that come as a surprise to a California patient, and there should be ease of access to HIE information in any locale. Also, individuals who are victims of medical identity theft need assistance in locating all of the places their records have been exchanged.

As such, we request that California commit to registering or listing all HIEs in California on a single page or website maintained by he state of California. CalOHII is already collecting certain information from HIEs; the cost to create and maintain a web page with this information for the public would be quite low, and would be of great service over the long term.

There is precedent for such activity. Currently, the Fair Credit Reporting Act (FCRA) allows consumers the right to access their credit reports and make corrections and to assert other rights granted under the law. Congress ultimately created a unified web portal, www.annualcreditreport.com, for consumers to exercise their FCRA rights in a simple interface largely due to the complexities and burdens involved in making consumers find and then go to each credit reporting bureau one by one.

We believe that similarly, Californians need a single web portal at the state level they can go to locate all California HIEs. We envision that Californians would be able to find contact information, the full HIPAA notice and privacy policy, and information about how to request a copy of their HIE information and other relevant details at the minimum. We also envision that Californians will be able to readily see and access all waivers granted to HIEs, including the details of why the waiver was granted and how long the waiver will be in place.

III. Medical ID Theft is a Substantial Issue in HIEs and Patients Need a System for Recourse

---

electronic HIE is to facilitate information sharing and exchange. Even when state laws allow for exchange without patient consent, most organizations do not exercise this option. In order to achieve any level of systemic durability and success, HIE efforts must establish trust relationships with all participants, including patients." Available at: http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__privacy_and_security/1147.

Medical identity theft is a known risk in health care systems, and electronic health care systems have been proven to facilitate the crime of medical identity theft in scope and breadth. Patients have encountered obstacles in removing incorrect information from their records after this crime; these obstacles can be even more overwhelming in the HIE environment. The World Privacy Forum has conducted and published a great deal of information about this crime,[9] as have others, including the FBI. The research is unambiguous: medical identity theft exists, and electronic health information exchanges pose a high risk for this crime. Unfortunately, unlike financial forms of identity theft, medical identity theft poses direct health risks to patients, and reputational risks to providers. It is crucial to patient trust and well-being that mitigation tools are in place in HIE projects at the outset.

Because of the risks medical identity theft poses, we request that California put in place a mechanism for patients to mitigate the problems that can result from this crime at HIEs. We suggest the following as first steps to mitigation for patients:

1. Revocation of consent mechanisms are crucial for victims of medical ID theft. **We recommend that there are no waivers for revocation of consent for this victim class**.
2. A mechanism for clearing fraudulent or incorrect information from an HIE is essential. Victims need a way to clearly know and understand where all copies of their patient data has been sent or resides, and they must have a way to remove these copies in their entirety in the case of incorrect patient information. (The core harm of medical identity theft is that patient files become inaccurate due to fraudulent or otherwise incorrect information.)
3. It would be useful for the state to develop a red flag alert for HIEs to use in the case of medical ID theft, similar to financial red flag alerts.
4. It would be helpful for California to have a written policy for HIEs on medical ID theft mitigation to ensure evenhanded treatment of victims. Jurisdictional boundaries are often crossed in medical ID theft cases, making mitigation more complex when differing policies and procedures are in place.

IV. The Waiver for Consent and Other Key Privacy Protections is Troubling and Should be Minimized and Monitored

The regulations state that some aspects of the regulations may be waived, including patient consent. We have many questions about this waiver process and are deeply concerned that this waiver process is a significant, substantial loophole in the proposed regulations.

1. There is no formalized procedure for the granting of a waiver. We do not see specific waiver guidelines, nor do we see any systematized method for reviewing

[9] See Dixon, Pam. *Medical Identity Theft, The Information Crime That Can Kill You*, World Privacy Forum, May 2006. http://www.worldprivacyforum.org/medicalidentitytheft.html .

waivers, nor specific benchmarks for reevaluating waivers after they have been granted. We request that a formal procedure be written and available for public comment prior to implementation.

2. **Patient consent should not be able to be waived.**
3. Waivers should be time-limited at a minimum, and should be reviewed at regular, prescribed intervals.
4. The waiver section of the proposed guidelines needs, in general, more thought and work. There needs to be at a minimum a set of formal procedures for the granting of a waiver. Waivers should not be an easy backdoor for HIEs to get out of regulations that protect patient privacy and security.
5. If a waiver is granted, this should be posted along with the HIE's other policies and information at the CalOHII website, at a minimum. The items that have been waived and the reason for the waiver should also be published. There should be no hidden waivers that California patients don't know about or have the ability to read and access. There must be adequate and even robust transparency in the HIE process.
6. The waiver process, if left as is, has the potential to undermine patient trust as the regulations could be undermined if too many waivers are granted, thus making HIEs less predictable and regular for patients to assess.

We urge the state great caution in the area of these waivers; if left as is, the waivers can potentially undermine the good the state seeks to establish with these regulations.

V. HIE Architectures Need to Be Broadly Construed

The idea behind HIEs is quite broad, and the vision for the future is equally broad: widescale, inter-regional, and interstate exchange of patient and other data between providers and others. We are concerned about narrowly defined versions of HIEs such as "direct HIE," and so forth, that do not define or envision HIE in a broad manner.

Privacy and security guidelines for California HIEs need to be broad in their vision so as to be applicable to as many HIE architectures as possible. In the early 1990s, the web architecture existed, and the possibilities were exciting. But no one conceived of a Facebook application to that web architecture until much later. Fortunately, baseline Internet protocols, underlying architectures, and policies were broad enough to allow for such innovation. Similarly, the privacy and security protocols for HIE need to have a broad vision that foresees the larger HIE picture and allows for core privacy protections in a multiplicity of environments. That is why patient consent is a core value that must be preserved in HIEs. It is also why granular patient consent should be left on the table for consideration as a future option as the HIE architecture matures.

While it is possible at the current time to so narrowly define an HIE that patient consent seems like it is minimized as a necessity, this strategy is shortsighted. We are quite sure that HIEs will take many forms and will surprise all of us with innovation. What must remain constant are the values of privacy such as patient consent and confidentiality,

among other rights and protections. California should not be lulled into such narrow definitions of HIE that it neglects to protect privacy in a multiplicity of formats both existing now, and to come in the very near future.

VI. Conclusion

We appreciate your interest in HIE in California, and we appreciate your consideration of this matter. We are happy to assist in the California HIE process, and welcome any questions or feedback you may have.

Sincerely,

s/

Pam Dixon
Executive Director, World Privacy Forum
www.worldprivacyforum.org

Jeffrey Chester,
Executive Director, Center for Digital Democracy
www.democraticmedia.org

Linda Ackerman,
Senior Counsel, Privacy Activism
www.privacyactivism.org