REPORT TO THE LEGISLATURE

DEMONSTRATION PROJECT SPECIFIC TO PATIENT CONSENT FOR HEALTH INFORMATION EXCHANGE

MARCH 2014

California Health & Human Services Agency

Office of Health Information Integrity

Table of Contents

Questions about this report should be directed to Cassie McTaggart at (916) 651-0422 or Cassandra.McTaggart@ohi.ca.gov.

Executive Summary

Recognizing the electronic exchange of health information has the potential to significantly improve the quality of treatment, reduce unnecessary health care costs, and increase administrative efficiencies within the health care system, the California Legislature in 2010 passed Assembly Bill 278, authorizing the California Office of Health Information Integrity (CalOHII) to administer Demonstration Projects. The purpose of AB 278 was to evaluate potential solutions to facilitate health information exchange (HIE) that promote quality of care, respect the privacy and security of personal health information, and enhance the trust of stakeholders. While there are many facets to the implementation of health information technology (HIT) and HIE, CalOHII focused on evaluating patient consent because in 2010 that was a critical issue facing the industry. Most states and the federal government have moved away from consent as *the* most important element for the privacy and security of HIE; however, California stakeholders are looking to the California Health and Human Services Agency to craft a solution to help move the industry forward. The recommendations developed through the Demonstration Projects provide the necessary guidance to propel current HIE efforts and outline the framework for the future state of the electronic movement of health information.

By evaluating consent through the Demonstration Projects, in conjunction with related activities conducted through the State HIE Cooperative Agreement Grant, CalOHII developed an assessment of what should be done based on the scope, as well as the constraints and challenges facing the industry. After an evaluation and analysis of the Demonstration Projects' findings, CalOHII recommends the following in order to advance the private and secure exchange of health information in California:

1. **Establish a common vocabulary and change the conversation** to reduce confusion with terminology, create a standardized language, and move away from patient permission as a single policy lever.
2. Continue to **let health information organizations determine the patient permission model** that is most appropriate for the community they serve.
3. **Patients must be provided an opportunity to make a meaningful choice** regarding the sharing of their protected health information.
4. **Technology solutions must evolve** to support granularity and electronic permission capture.
5. **Governance of interoperability is needed to sustain efforts.**

CalOHII would specifically like to thank our demonstration partners, San Diego Regional Health Information Exchange, Santa Cruz Health Information Exchange, and Inland Empire Health Information Exchange, and our statewide stakeholders for their patience and support while demonstration projects were ongoing and recommendations were under development.

Introduction

The California Health and Human Services Agency (CHHS) is the State's lead agency on health information exchange and health information technology ("eHealth") under Title XIII of the 2009 American Recovery and Reinvestment Act (ARRA), subtitled the Health Information Technology for Economic and Clinical Health Act (HITECH). Thus, CHHS has broad responsibility and oversight for administering the federal State HIE Cooperative Agreement Grant Program[1], the Medi-Cal Electronic Health Record Incentive Program in the Department of Health Care Services (DHCS), and regulatory development and enforcement pertaining to security and privacy of health information.

The California Office of Health Information Integrity (CalOHII) is an office within CHHS providing policy guidance and support to ensure that health information can be shared with the patient, the patient's providers and other key stakeholders in accordance with state and federal law. CalOHII's primary statutory authority is to assume statewide leadership, coordination, policy formulation, direction, and oversight responsibilities of implementation of the Health Insurance Portability and Accountability Act (HIPAA) among state departments.[2] Under the direction of the Deputy Secretary for HIE, CalOHII also provides oversight of the eHealth initiatives and is charged with coordinating eHealth activities both within State government and between non-governmental eHealth partners.

To carry out the programmatic aspects of the federally-funded $38.8 million State Health Information Exchange Cooperative Agreement grant, the Deputy Secretary and CalOHII have worked in concert with the University of California Davis, California Health eQuality (CHeQ), under an inter-agency agreement. Specific federally-defined roles for the State include developing necessary technical and trust standards and agreements; providing grants to local health information organizations (HIOs); removing barriers to HIE interoperability; coordinating with Medicaid and public health programs to support meaningful use and population health management; and convening and informing HIE stakeholders.

Lastly, Assembly Bill 278 (Monning, Statutes of 2010) authorized CalOHII to administer Demonstration Projects to evaluate potential solutions to facilitate health information exchange (HIE) that promote quality of care, respect the privacy and security of personal health information, and enhance the trust of stakeholders.

[1] Office of the National Coordinator, State Cooperative Agreement Program, www.healthit.gov

[2] Passed in 1996, HIPAA made comprehensive changes to healthcare including providing the ability to transfer and continue health insurance coverage when individuals change or lose their jobs (portability), industry-wide standards for electronic billing, and privacy and security of health information.

Background

Health information exchange is defined as the capability to electronically move health information among disparate healthcare information systems while maintaining the integrity of the information being exchanged. The term HIE is used to describe both the process of exchanging health information electronically, and the organization or entity overseeing and governing the exchange. Such entities may also be referred to as health information organizations (HIOs), health information networks (HINs), or health information service providers (HISPs). The primary goal of exchange is to facilitate access to, and retrieval of, clinical data to improve the quality, accessibility, and cost-effectiveness of healthcare.

Privacy and security policies related to the electronic exchange of health information have been the subject of intense deliberations both nationally and within California, and none more so than patient consent for HIE. One of the foremost policy challenges related to the electronic exchange of health information has been whether – and to what extent how – individuals should have the ability to exercise control over their electronic health information. A variety of consent models exist and can be applied in different contexts of exchange, with further variation depending on the level of granularity allowed.[3] These models of consent generally apply to participation in a networked electronic exchange effort – meaning among unaffiliated organizations – and are not intended to constrain the usual transmission of information for treatment, payment, or health care operations as permitted under HIPAA and other relevant state and federal laws.

The most common consent options are:

- No consent – health information of patients is automatically shared; patients exercise no choice;
- Opt-out – default is for health information of patients to be shared, but the patient may opt out completely;
- Opt-out with exceptions – default is for health information to be shared, but the patient can opt out completely or allow only select data to be shared, i.e. in an emergency;
- Opt-in – default is that no patient health information is shared; patient must actively express consent to be shared, but if they do so then their information must be all in or all out;
- Opt-in with restrictions – default is that no patient health information is made available, but the patient may allow a subset of select data to be included or in certain situations, i.e. in an emergency.

In a *no consent* model, electronic exchange can take place irrespective of and without obtaining patient preferences for participation (within the bounds of applicable federal and state laws).[4] Patients and consumer advocates tend to prefer *opt-in* models because patients retain some level of control with respect to how their health information is used and exchanged. Conversely, providers favor *opt-out* models of exchange because they assume it gives access to health information for a larger number of patients.

The HIPAA Privacy Rule serves as a floor for privacy protections, allowing covered entities to access, use, and disclose protected health information (PHI) without first obtaining a patient's authorization for

[3] Melissa Goldstein and Alison Rein, "Consumer Consent Options for Electronic Health Information Exchange: Policy Considerations and Analysis", March 2010, p. ES-1
[4] *Id.,* p. 6

purposes of treatment, payment, and health care operations,[5] as well as certain other circumstances, such as for public health reporting and certain law enforcement purposes. Most experts acknowledge that allowing information to be shared among health care entities without requiring prior consent for a set of core health functions – and requiring authorization for uses and disclosures that are not part of this health care "core" – is good public policy and protects privacy.[6] However, there is also general agreement that patients should have some control over their health information and how it is used and disclosed, although the ideal reach of that control is less clear.

At the national level, a majority of states have chosen to adopt a uniform consent policy for HIE, in line with early efforts by the Office of National Coordinator for Health Information Technology (ONC); the ONC Health Information Technology Policy Committee made recommendations in 2010 that outlined a comprehensive framework of sound and practicable policies for privacy, security, and patient consent but related solely to treatment.[7] Building upon fair information practices and patient expectations based on the trusted patient-provider relationship, the HIT Policy Committee recommended that "meaningful consent" – whether opt-in or opt-out – be required when the provider no longer has control over how the patient's information is used and disclosed, such as with a query-based model of exchange.[8] In circumstances where the provider maintains control over uses and disclosures of protected health information – such as directed exchange – consent for treatment, payment, and operations is not required beyond what is currently required in law (i.e. authorization for sharing sensitive health information).

Since 2007, California has been working on developing privacy and security standards for electronic health information exchange. The California Privacy and Security Advisory Board (CalPSAB), comprised of industry stakeholders, was formed to develop and recommend new policies and standards related to the privacy and security of health information. Through the stakeholder process, CalPSAB developed a set of principles for fair information practices to establish the foundation for trust in the exchange of an individual's health information.[9] The "Principles for Fair Information Practices" outline the core expectations and minimum criteria that should govern the design and implementation of health information exchange and technology in California.[10] CalPSAB attempted to develop a uniform consent policy for California; however a lengthy deliberation process bore no clear outcomes or consensus. In December 2010, the board voted to proceed with an opt-in model for California and sent an informational letter to incoming CHHS Secretary Diana Dooley, reporting on the work done by the group and the consent policy recommendations.

There continued to be controversy over the outcome of the CalPSAB board vote to adopt an opt-in consent model. In developing the regulations for the Demonstration Projects, CalOHII chose to require

[5] 45 C.F.R §164.502
[6] Center for Democracy & Technology, "Rethinking the Role of Consent in Protecting Health Information Privacy", January 2009, p. 5
[7] Health Information Technology Policy Committee, Recommendations of the Privacy and Security Working Group, September 2010
[8] Refer to Appendix A, p.22 of this report for more information about the different types of health information exchange and the models of governance.
[9] Consumers Union et al, "Consumer and Patient Principles for Electronic Health Information Exchange in California", June 2010
[10] California HealthCare Foundation, "Achieving the Right Balance: Privacy and Security Policies to Support Electronic Health Information Exchange", June 2012, p. 6

Participants to have an affirmative (opt-in) consent policy, with a waiver process allowing for a Participant to test alternative consent models. Feedback received from stakeholders during the development of the Demonstration Projects Regulations highlighted continued opposition to an opt-in consent policy for the Demonstration Projects.[11] Following the elimination of CalPSAB, collaborative efforts of stakeholders continued through the CalOHII Privacy and Security Steering Teams,[12] which identified specific policy areas to be tested through the Demonstration Projects. While the Demonstration Projects allowed CalOHII to test a variety of privacy and security policies, it was recognized that one of the most important elements in promoting interoperable health information exchange continued to be patient consent.

CalOHII released a Request for Applications (RFA) in January 2011 to evaluate HIE privacy and security policies, address the feasibility of implementation, and gauge the implementation impact. Applicants were invited to "propose comprehensive implementation strategies for the identified demonstration project"– i.e. affirmative consent.[13] Following an extended selection process, two proposals were selected and demonstration projects were awarded to San Diego Beacon eHealth Community (SDBC)[14] and Western Health Information Network (WHIN). Both Participants planned to test opt-in consent across a broad spectrum of health care stakeholders. (Refer to Appendix C for a detailed description of the SDBC Demonstration Project.) A signed Memorandum of Understanding was finalized between WHIN and CalOHII in March 2012. However, shortly thereafter, WHIN ceased operations and submitted a notice of termination, effective July 2012, as a Participant of the Demonstration Projects.

During this time, CalOHII experienced a change in executive leadership. The need for a more robust evaluation of consent to allow for a true comparison of various consent policies was recognized. CalOHII released a second RFA in August 2012 to test a broad array of consent models. Two health information organizations submitted responses to the new RFA, both proposing to test an opt-out consent policy – Inland Empire Health Information Exchange (IEHIE) and Santa Cruz Health Information Exchange (SCHIE) (Refer to Appendix D and E, respectively). Combined with the opt-in consent Demonstration Project with SDBC, CalOHII had three unique Demonstration Projects to evaluate patient consent for health information exchange.

It should be noted that while the governance model of each HIO impacts how it will use and disclose protected health information and the consent model implemented, those variances were not taken into consideration with these Demonstration Projects. For a broader discussion on HIO governance models and how consent is impacted, refer to Appendix A. Additionally, CalOHII Demonstration Projects were able to test some aspects of existing state and federal law, such as the development of technical and administrative safeguards, and interpret or clarify ambiguous terms and phrases in the law for state departments, but CalOHII does not have authority to create new state law or override existing state law for all entities in California. Therefore, CalOHII limited the scope of the Demonstration Projects to evaluating policies regarding patient consent for HIE, specifically the administrative process of obtaining patient permission to participate in HIE.

[11] Consumers Union and Center for Democracy & Technology joint letter to CalOHII, November 2011
[12] The Privacy and Security Steering Teams are now the Policy Steering Team.
[13] CalOHII Request for Application for Health Information Exchange Demonstration Projects, January 2011
[14] SDBC transitioned to a new non-profit organization in 2012, known as San Diego Regional Health Information Exchange. Refer to Appendix C for more information.

Evaluation of Demonstration Projects

To effectively evaluate the various consent models, CalOHII worked with Dr. Robert Miller, an Independent Evaluator from the University of California, San Francisco, to outline the Demonstration Project objectives, what would be tested, and how the objectives would be measured. Because of the size and complexity of the consent issue and the lengthy deliberations, there were numerous options for evaluating consent. Rather than evaluating the merits of one consent model or another, CalOHII focused on measuring and identifying specific implementation issues pertaining to the process of obtaining patient consent for the electronic exchange of their health information.

The primary objectives of the Demonstration Projects, as specified in AB 278 (Monning, Statutes of 2010), were to:

1) Identify barriers to implementing health information exchange (HIE);
2) Test potential privacy and security policies for the safe and secure exchange of health information, including, but not limited to, issues related to access to, and storage of, individual health information; and
3) Identify and address differences between state and federal laws regarding privacy of health information.

The objectives were also to increase transparency and knowledge of the use of health information and build a set of requirements for HIE that can evolve as technology evolves. The policies and procedures identified and created by the Demonstration Projects provide the framework necessary to promote further development and deployment of privacy-enhancing technologies while ensuring compliance with state and federal laws mandating the confidentiality of individual health information. The specific goals of the Demonstration Projects were to determine the operational feasibility of implementing the consent policy; discover issues associated with the operationalization of the policy; and develop and propose policy solutions.

In addition to quantitative data – i.e. number of patients seen and/or notified of the consent policy, number of patients opting-in or opting-out, etc. – the evaluation aimed to gather qualitative data such as patient satisfaction with the consent process and education, as well as provider satisfaction with the consent policy and processes. Through these Demonstration Projects, CalOHII hoped to understand the benefits and costs of the consent policy being tested and the impact on patient trust and engagement. Specifically, the Demonstration Projects aimed to evaluate such things as:

- The impact of the informed consent process on consumer confidence with HIE;
- Administrative impacts on different types of healthcare providers such as large integrated health systems, individual practices, clinics, labs, etc.; and
- Identification of technical solutions that support the policies.

The design of the data collection methodology, specific data elements, and evaluation criteria was a collaborative effort between CalOHII, the Independent Evaluator, and the Participants. The evaluation consisted of a set of quantitative data[15] submitted monthly, in addition to patient and provider surveys, monthly status meetings with Participants, and in-person and telephone interviews with clinic staff. The Demonstration Projects successfully gathered data and provided insight into the challenges of

[15] Refer to Appendix F for specific reporting requirements of the Demonstration Project Participants.

implementing a meaningful consent process, as well as identified potential solutions to overcoming those challenges.

Challenges

A variety of issues presented challenges to CalOHII and the Participants throughout the course of the Demonstration Projects. Many of the challenges stemmed from delays with the HIOs onboarding participating organizations, limited data collection, and an industry still in the formative stages. CalOHII held routine meetings with the Participants and Independent Evaluator to identify gaps and to mitigate the challenges. Additionally, CalOHII routinely met with stakeholders, who provided valuable input and guidance for the Demonstration Projects.

The primary challenge was the fact that the health information exchange industry is, in many ways, still in its infancy. A majority of HIOs in the state are in the planning stages or in the early implementation stages.[16] Many either have not fully defined their consent policies and processes or are not far enough along with participating organizations to begin testing the consent model. While it is critical to fully outline the consent policies and procedures during the planning phases, some Participants made policy decisions as work progressed. IEHIE had executed agreements with several participating organizations and defined a consent policy, but many of the HIO's participating organizations were in different phases of actually sharing data. Some clinics participating in the Demonstration Project chose not to begin the patient notification process until they were ready to actually share data, which meant they were unable to submit consent data to CalOHII.

Likewise, in the case of San Diego Regional Health Information Exchange (SDRHIE),[17] the organization went through a governance transition, resulting in a restart of operations. The Beacon[18] grant and HIO operations were previously being managed by the University of California, San Diego; in January 2013, the work was transitioned to a new non-profit organization, which meant that new participant agreements, policies, and procedures had to be completed. While some aspects of the HIO continued to operate, others such as consent management were on hold until after the transition was complete. These external forces impacted the Demonstration Project and impeded the amount of data collected.

Data collection in general was also a challenge throughout the projects. CalOHII worked with the Independent Evaluator to create a set of reporting requirements and baseline information to be collected from each Participant, but it was discovered early that Participants were not able to provide much of the requested data for various reasons, most notably system limitations. For example, CalOHII set out to measure the number of patients opting out of sharing their health information against the actual number of patients offered the choice (which may or may not be the same as the number of patients seen). IEHIE does not have access to clinic schedules and therefore did not have the precise number of patients that presented for a visit; in addition, IEHIE does not track the number of patients who were offered the choice to participate, only how many patients actually opt out – in this case, none

[16] See Appendix B for a map of the health information organizations in California.
[17] See footnote 14
[18] The San Diego Beacon eHealth Community (now known as San Diego Regional HIE) was one of 17 communities selected by the ONC to receive a grant to build and strengthen health IT infrastructure and exchange capabilities; reduce costs while improving quality and population health; and test innovative approaches to care delivery, performance measurement, and technology integration. For more, see http://www.healthit.gov/policy-researchers-implementers/beacon-community-program.

during the course of the Demonstration Project. Although the amount of data available to be analyzed was severely limited during the Demonstration Projects, CalOHII collected a wealth of non-quantitative data that helped shape the evaluation findings and recommendations. This information included qualitative information on the consent management process, provider experience with and implementation of the consent policy, and site visits and telephone conversations with the Participants to discuss challenges and potential areas of improvement.

A final challenge to the Demonstration Projects was that CalOHII does not have authority to govern HIE or to create regulations governing consent for the electronic movement of health information. For many years, most notably since the elimination of CalPSAB, California stakeholders have been asking for direction, but CalOHII is limited in its capacity to provide guidance to the industry. This challenge somewhat minimized the outcomes CalOHII could develop from the evaluation, specifically in terms of enforcement. Despite numerous requests from HIO leaders and industry stakeholders for a single consent solution in California, CalOHII does not have the authority to provide such direction, nor create the regulations needed. At best, CalOHII can provide guidance, recommend best practices for HIOs in the state, and provide tools to help with implementation. However, CalOHII also found through the course of the Demonstration Projects that a single consent policy may not be the most appropriate solution for California, as the industry as a whole has progressed to recognizing that consent is only one element to building trust and securing health information; this helped mitigate any challenges lack of authority may have presented.

Findings

Consent has long been an issue in California, with stakeholders often divided about how to promote and enhance the electronic movement of health information while still protecting Californians constitutional right to privacy and ensuring the safe and secure sharing of critical data. By focusing on consent through the Demonstration Projects, CalOHII sought to evaluate different ways that health information organizations implement consent policies, as well as the opportunity to identify best practices for informing patients of uses and disclosures while lessening the administrative burden on providers and identifying ways to improve the process. Findings of the Demonstration Projects are:

1. Lack of standard, consistent terminology is a barrier to successful HIE.
2. When offered the choice, patients generally agree to share health information electronically.
3. Previously-held beliefs about the consent management process may not be true.
4. EHR and technology standardization is a barrier to electronic consent management.
5. Lack of standardization among HIOs is a barrier to interoperability.
6. Trust remains a critical component to successful HIE.

1. Lack of standard, consistent terminology is a barrier to successful HIE

The laws and regulations that govern HIE and the sharing of health information are numerous and convoluted. A major finding of the Demonstration Projects is a distinct and widespread misunderstanding of state and federal laws regarding patient consent for HIE. Additionally, terms and vocabulary are not standardized, are confusing, and are used interchangeably. For example, consent can refer to consent for treatment or consent for HIE. Patients have a tangible understanding of what consent for treatment means – if they sign or give permission, the doctor will provide care. However, consent for HIE is more abstract and thus harder for patients to understand the direct impact and value to them.

The terms consent and authorization are often – and inappropriately – used interchangeably, partly because they have come to mean similar things, but also because state and federal privacy law definitions are not aligned. For example, the HIPAA Privacy Rule defines authorization in very specific terms and states that protected health information may be shared for treatment, payment, and healthcare operations without prior authorization. Conversely, HIPAA does not specifically define consent, but states that organizations *may* require prior consent before sharing information for treatment, payment, or operations. Guidance from HHS defines consent as written permission from individuals to use and disclose their health information.[19] Additional laws and regulations specify when consent or authorization is required, such as when sharing information related to substance abuse treatment. Under California law, the term authorization is defined under the Confidentiality of Medical Information Act (CMIA) as "permission granted…for the disclosure of medical information".[20] Conceptually, consent and authorization accomplish the same goal which is ensuring that an individual agrees to particular uses and disclosures of their health information.[21] However, the misalignment of laws and definitions, the highly-charged issues related to patient consent, and the misrepresentation of the terms continues to present a critical challenge to the development of privacy and security policies.

Another challenge with terminology relates to the terms opt-in and opt-out. In technology terms, opt-in and opt-out refer to the state of the data as it exists in the system, e.g. in an opt-in system the patient data is stored but cannot be shared until the "switch" is turned on, which happens once the patient has given permission. However, the industry has adopted the terms to mean the process by which permission is granted by the patient. The misuse of these common terms presented challenges even when attempting to describe the various policies and procedures each of the Participants implemented. Stakeholders frequently disagreed on describing the SCHIE consent policy as opt-out, stating it wasn't a true opt-out model because the HIO collected signatures from each patient that was notified of their inclusion in the health information exchange.[22]

Most other states have not had the same challenge because they instituted singular consent policies, supported by state law. However, California efforts in this area have stalled due to the highly-charged and polarizing nature of the consent debate. In order for HIE efforts to continue in California, CalOHII has identified a critical need to standardize the terminology to describe patient permission to share their health information electronically and the system conditions for managing patient consent.

2. *When offered the choice, patients generally agree to share health information electronically.*

A major finding of the Demonstration Projects was that, when offered the choice at the point of care, a large majority of patients – approximately 95% – elect to participate in electronic health information exchange. This finding was true for both opt-in and opt-out models, which was unexpected because there is a general belief that opt-in models do not result in higher rates of participation. For example, Rady Children's Hospital, part of SDRHIE, implemented an affirmative (opt-in) consent process in July 2012. Patients were educated about HIE at the time of care and were given the opportunity to opt-in. In just over nine months, Rady Children's Hospital achieved a 95% opt-in rate and consented approximately 97% of the active patient population.

[19] Office of Civil Rights Privacy Brief, Summary of the Privacy Rule, p. 5
[20] California Civil Code § 56.05
[21] CDT, *supra* note 6, p. 23
[22] Refer to Appendix E, p. 37 for more information on the SCHIE consent policy and processes.

Participants testing an opt-out consent model also saw an overwhelming number of patients electing to participate in their community health information organization. SCHIE tested an opt-out process with patient notification. Patients were presented with education material at the point of care by clinic staff and informed of their right to opt-out. During the evaluation period, less than 1% of patients chose to opt-out. Likewise, IEHIE saw no patients choosing to opt-out of HIE during the evaluation period.

The Demonstration Project data is consistent with data from health information organizations throughout the country. Kansas Health Information Exchange implemented an opt-out process for the health information exchange in June of 2012 and in the first few months saw an opt-out rate of less than 1%. Nebraska Health Information Initiative – regarded as one of the most advanced HIEs in the country in terms of successfully implementing an opt-out model – has a 2-3% opt-out rate.[23] Conversely, the Massachusetts eHealth Collaborative, which implemented an opt-in consent model, reported that more than 90% of patients gave permission to have their data shared.[24]

Although this finding is in contrast to other studies on patient preferences that found patients prefer an opt-in model, it is important to understand the context of each of the studies, particularly when comparing with the Demonstration Project findings. As an example, the consumer consent preferences survey (discussed in more detail later in this document) found that Respondents preferred an opt-in model for sharing health information. However, this survey was not conducted at the point of care. Surveying in a hypothetical context allows consumers to consider a variety of options conceptually. Conversely, the Demonstration Project evaluation was based on patient preferences in a "real world" setting, captured at the point of care, with limited choice options – patients either agree to share their information or not with no granularity. Additionally, patients were presented with the opportunity to discuss the benefits and risks with their health care professional in order to make a more informed choice, unlike the Consumer Preferences Survey, which focused on specific questions and circumstances. Refer to Appendix A for more information on the Consumer Consent Preferences Survey conducted by the University of San Francisco.

3. Previously-held beliefs about the consent management process may not be true

A primary goal of the Demonstration Projects was to evaluate the administrative burden of the various consent models in order to understand the barriers to offering consent to patients. One of the concerns providers have previously voiced is the increased perceived financial and administrative burden associated with initiating and maintaining a consent management process. A common notion is that an opt-out consent model requires a different level of administrative effort and therefore is preferable because the patient data is available by default. On the other hand, an opt-in model requires upfront work to achieve high rates of participation and significant patient data. Findings from the Demonstration Projects indicate that these previously-held beliefs are not necessarily true and that a variety of factors can affect the impact of implementing a consent management policy and process, regardless of whether an HIO is opt-in or opt-out.

Providers typically want three elements when participating in electronic health information exchange: 1) consistent and comprehensive access to information; 2) an assurance that using electronic exchange won't increase their exposure to liability; and 3) minimization of technical, financial, and administrative

[23] Telephone call with Nebraska Health Information Exchange, January 2013
[24] Ken Terry, iHealthBeat, "Patient Consent for Information Exchange Comes Into Focus", November 2012

burdens.[25] Each of the consent models evaluated had a policy by which they educated patients and gave patients an opportunity to choose whether to participate in the exchange of health information or not; however the actual level of effort and impact to workflows varied depending on how the process was implemented. The actual participation rates were relatively high regardless of the consent model chosen by the HIOs – in the upper 90th percentile; however, this level of achievement requires a tremendous level of awareness and trust building, as well as education.

SCHIE implemented an opt-out with notification process, where the consent status in the system was set to "none" for all patients until they were informed about HIE and given the opportunity to opt-out at the time of care (i.e. during an office visit). Every patient signed an attestation that acknowledged this notification, as well as their right to opt-out of the HIE. Each participating clinic had slightly different processes, but most relied on the HIE administrator (SCHIE) to gather the attestation forms and enter the information in the HIE. In a report to CalOHII, SCHIE states "obtaining [a] hard copy/paper consent form for consent to exchange electronic health information is a conflict in itself. Practices manually updating two systems, HIE updating consent status on behalf of practices are extremely time consuming, and not all forms were complete or legible".[26] The participation rates were high and only a few patients opted out of the system, but the process required significant work on the part of the HIE administrator. It should be noted providers believed the effort was important to building trust and engaging patients in health information exchange. SCHIE has been in operation for over a decade and most patients already had information in the HIE; however, SCHIE implemented the notification process to build patient trust and reduce the risk of liability.

Inland Empire HIE also implemented an opt-out consent model, but had a streamlined notification process, whereby patients were mailed an education pamphlet with instructions on how to opt-out of sharing health information. Participating providers did not require any form of signature or attestation from the patient that the education was provided or that they acknowledged how their data would be shared by default. While this type of consent management process is less of an administrative burden and produced high participation rates in the HIO – no patients chose to opt-out during the evaluation – there may be a false sense of trust by the patient and potentially skewed participation rates because there is no way to verify that patients received the notice and were truly comfortable with their data being shared.

SDRHIE is a federated model of exchange[27], with a central policy of opt-in consent for sharing patient data through the HIO. Rady Children's Hospital was the only participating SDRHIE organization that had fully implemented an opt-in consent management process during the course of the Demonstration Projects. Rady Children's Hospital implemented an opt-in consent policy, with patient education and affirmative consent being captured at the time of care by incorporating the patient consent for HIE into the existing registration process; by doing so Rady's reported that very little additional resources were expended – an estimated additional time spent of approximately one minute per patient.[28] Although SCHIE and Rady Children's Hospital had similar approaches and both educated patients in advance, Rady's attributed their low impact on workflows to reliance on existing business processes, the unique

[25] Goldstein, *supra* note 3, p.25
[26] Santa Cruz Health Information Exchange, Consent Demonstration Project Report, p.7
[27] Refer to Appendix for a description of the different models of health information exchange.
[28] Telephone call with Rady Children's Hospital, April 2013

nature of the patient population, a higher level of trust, the strong C-suite level support for HIE, and changes to policies and processes to support HIE.

While each of the Participants had similar consent management policies, the Participants' implementation of that policy varied; the variances had either minimal or significant impacts to workflow. It is also important to note that the cultural reliance on paper is in direct contradiction to the promotion and advancement of health information technology as a means to improve the healthcare system. In general, technology has not evolved within healthcare to collect electronic signatures and remove the burden of collecting paper forms. Limited testing has occurred on e-consent systems, but a vast majority of HIOs across the country use paper forms to track patient permission and manually update the patient's consent status in the electronic health record (EHR) or HIE software.

4. EHR technology standardization is a barrier to electronic consent

Although the Participants achieved high rates of participation, regardless of the consent model implemented, the paper-based process placed significant burden on the providers and the HIOs. One of the biggest barriers to widespread adoption of HIE and true interoperability is the lack of standards, specifically, the inability to manage consent in EHR systems. For each of the Participants, the lack of a consent status field within the EHR was an issue, because that meant the participating organizations had to separately access the HIE platform in order to view the patient's current consent status. And even if the consent status was stored in the EHR, the process of updating the consent status in the HIE platform was not universally automated.

For example, Rady Children's Hospital uses an EHR vendor that stores the consent status in the actual electronic record and transmits the consent status to the HIE via an electronic message. However, both SCHIE and IEHIE participating organizations do not have EHR's with this capability and the consent status is updated manually either by the provider or the HIO administrator. According to SCHIE, this creates silos of information; they are currently working on solutions, including electronic signatures and bi-directional interfaces.[29] However, the cost of hardware and interfaces along with EHR vendor development timetables are a barrier for many providers.[30]

Another critical finding is that the current systems do not support granularity – permissions are set to the patient's information is "all in" or "all out". Numerous state and federal laws set patient authorization requirements based on the type of data being shared (i.e. mental health, substance abuse treatment, HIV/AIDS, whether the patient is a minor and may make their own medical decisions) or who the receiving party is of the data – public health department, employer, etc. Current EHR and HIE systems do not support data segmentation[31] or the ability for patients to designate at a granular level what information or which providers they want to restrict. Due to these limitations, HIO's are creating "all in" or "all out" situations, where the only way to restrict certain types of information from being shared is to opt out of sharing all health information. In the case of SDRHIE, the participating organizations filter data at the EHR level by setting controls on patient records to not allow them to be

[29] An interface is generally a combination of the hardware connection between two systems and the software they use to communicate. An example is a printer, where the USB or network cable connects the user's computer to the printer and the printer driver tells the computer how to communicate to the specific printer. In healthcare, the actual connection is typically through virtual private network (VPN) connections, etc.
[30] Santa Cruz HIE, *supra* note 27
[31] Data segmentation is the process of sequestering from capture, access or view certain data elements that are perceived by a legal entity, institution, organization or individual as being undesirable to share.

shared via the HIE system. Additionally, Rady Children's Hospital creates a separate medical record for minors with sensitive health information to conform to laws that permit minors to make certain medical decisions. While these workarounds help ensure privacy, they hamper the purpose of health information exchange, which is ensuring the right information flows to the right place when and where it is needed for patient care.

5. Lack of standardization among HIOs is a barrier to interoperability

Another important finding of the Demonstration Projects is that all health information organizations in California – and across the country – are not created equally. Patient demographics, internal governance, service area/locations, and provider demographics all impact the implementation of a given consent policy and process. Each HIO in the Demonstration Projects implemented consent management in slightly different ways, even when choosing the same consent model. SCHIE implemented a consent management process that was uniform across all participating sites, with the variation only in how clinics notify the patients. IEHIE took a hands-off approach, which follows their governance model, and allowed each site to implement the opt-out consent model as it deemed appropriate. SDRHIE implemented a hybrid consent model, which follows the decentralized approach to governance in that community. Each participating organization in the HIO set its own consent management process and managed consent at the local level. For example, Rady Children's Hospital has an opt-in consent policy, but Kaiser Permanente[32] has an opt-out consent policy across its healthcare system.

The type of model the HIO operates may play a role in determining the consent model, since the expectations of the patient may be different. While the Demonstration Projects did not specifically evaluate the technical aspects of HIE, the impact of which HIO model the organization adopts may play a role in the consent model chosen, and therefore presents a challenge to policymakers because of the complexity of the industry, as organizations and providers are burdened with educating and engaging patients in the permissions process. Refer to Appendix A for more information on the different types of HIO governance models and the impact on consent policies.

6. Trust remains a critical component to successful HIE

Trust is a critical component in making health information exchange successful – patients must trust the providers to hold data securely and share it only when necessary; providers must trust one another to share relevant and accurate patient data; providers and patients must trust health plans to utilize health information appropriately; and all stakeholders must trust government entities to collect and hold only data needed for population safety and health.

One important finding from the Demonstration Projects was the lack of trust in many areas which may hinder the establishment of patient consent policies. In San Diego, the lack of trust – or fear of competition – made the widespread adoption of the community HIE difficult. The region includes several health systems that compete for patients, and although the organizations believe in the value of health information exchange, they have been slow to sign on to the community HIE. Some entities view patients and their data as key assets and feel that this data liquidity may make it easier for a patient to

[32] Kaiser Permanente did not participate in the consent Demonstration Project; however, as a participating organization in San Diego Beacon Community (predecessor to San Diego RHIE), information on how it shares data through the exchange was provided to CalOHII.

switch to a competitor.[33] This lack of trust makes the business case for HIE more difficult and, in turn, places consent management low in priority for the participating organizations.

However, trust proved to be a positive factor for some Demonstration Projects. Because SCHIE has been established for over a decade and the providers in the community have been sharing patient information for some time, there exists a high level of trust among providers, stakeholders, and patients. Patients in the community trust their providers and as such were more willing to participate in the exchange, which is exhibited by the extremely low opt-out rate of less than 1%. This can also be attributed to the power of default, which essentially means that individuals are generally inclined to follow whatever default option exists – whether opt-in or opt-out. Researchers have found that patients may believe that defaults are actually suggestions by the policy maker.[34] In the case of SCHIE, where patients have a high level of trust in their providers, the power of default may explain why patients tended to remain in the system, causing high participation rates. In an opt-in environment, the power of default may be a contributing factor to the lower participation rates typically seen with opt-in models, as patients may view the default of not sharing patient data without express patient permission as an influence by the provider. In difficult and stressful situations, many people choose to avoid decision making altogether and accept the status quo.[35] In either case, the power of default is an important element that stakeholders must consider when developing policies and procedures for engaging patients.

Conclusion

Preserving confidence in the individual health information contained in electronic health records and the information systems that protect and connect them is fundamental in achieving the goal of improving health care safety and efficiency. Comprehensive privacy and security protections and fair information practices create the public trust necessary to adopt health IT widely and achieve the benefits of HIE across California. The principles make it clear that it is not a choice between privacy and better health care – HIE initiatives should aim to achieve both.

The purpose of the Demonstration Projects was to evaluate potential HIE solutions that promote quality of care, respect the privacy and security of health information, and enhance the trust of stakeholders. Building and preserving trust in the electronic movement of health information requires leaders and policymakers to implement the entire complement of fair information practices, rather than relying on a single element – such as consent – to ensure patient information is available when and where it is needed for care, while ensuring that the data is protected and exchanged under strict medical privacy and confidentiality standards and procedures.

In order for health information exchange to be successful, trust relationships must be established with all participants, including patients. Patient engagement and education is critical – patients must understand what parts of their health information can be accessed and shared, who has access to their information, how information is protected, why information might be shared, and their choices in deciding what information is shared or not shared[36]. Consumer engagement is more than a buzzword –

[33] Robert Miller, PhD, "Report to ONC: Evaluation of the State HIE Program Award to California", January 2014, p.9
[34] Goldstein, *supra* note 3, p. 52
[35] Goldstein, supra note 3, p. 53
[36] Office of National Coordinator for Health Information Technology, http://www.healthit.gov

it is a critical element to fostering trust and encouraging participation, while meeting the Triple Aim[37] of healthcare – better care and better health at lower costs.

Numerous studies show that patients overwhelmingly prefer to be informed in advance of their information being shared. The ONC, in its eConsent Trial Project, found that patients are interested in learning more before they decide whether or not to allow health care providers to access or share their health information electronically[38]. While patients believe in the value of health information technology and the benefits of health information exchange, they also want to be assured of the privacy and security of their health information. However, offering patients the choice to participate in electronic health information exchange does not equate to patients choosing not to participate – the Demonstration Project evaluation shows that when offered the choice, a large majority of patients will choose to share their health information.

Generally speaking, state and federal laws permit health information to be shared among providers for treatment purposes. HIPAA provides a baseline of privacy protection; other state and federal laws require health care providers and business associates to obtain written authorization from the patient prior to disclosures of some health information. These privacy laws typically relate to disclosure of "sensitive" health information, i.e. substance abuse treatment, HIV/AIDs, etc. The rules become more complex as they describe the type of health information being shared and who is making the disclosure. Most electronic exchange models are unable to support this level of granularity because of the complexities with various state and federal laws and regulations, as well as the technical and procedural challenges associated with data segmentation[39].

Currently, HIOs approach consent as an "all in" or "all out" model of exchange, where patients who choose to participate do so knowing that all of their health information is available to be shared, including sensitive health information. Without a meaningful opportunity to restrict data, individuals with heightened concerns about having their health information accessible through a HIO have little recourse other than to choose not to share[40]. Some HIOs exclude sensitive health information from the exchange, filtering the data at the provider EHR level before it enters the HIE environment. However, these solutions do not help to promote health information exchange, since care coordination may be compromised by providers' inability to get the full picture of the patient's health information. Additionally, protected health information will be shared for permitted purposes by other means, i.e. fax, telephone, secure or encrypted email, which adds to patient confusion. While much of the focus on HIPAA has been related to privacy, it is critical to remember that the goal of HIPAA was to establish standards and operating rules that facilitate the use of electronic transactions by creating greater uniformity in data exchange and reducing reliance on paper forms and manual process – in other words, making health information portable. HIE is an evolution of HIPAA because it institutes practices that promote accountability, privacy and security for the electronic movement of health information.

Interoperability began as a concept and has evolved into HIE implementations that, in California, are privately driven and publicly assisted. Public assistance has included such initiatives as providing a

[37] The Triple Aim is a framework developed by the Institute for Healthcare Improvement that describes an approach to optimizing health system performance. http://www.ihi.org
[38] Kathryn Marchesini and Joy Pritts, "Meaningful Consent in Electronic Health Information Exchange: A Technology-Centric Approach", September 2013, http://healthaffairs.org/blog
[39] Goldestein, *supra* note 3, p. 9
[40] CDT, *supra* note 6, p. 16

governance model that supports allowing HIOs to function in accordance with business needs, grants to build HIE infrastructure, and legislative changes to allow flow of information within the law. However, there are still critical needs for public assistance. Lack of standards pervades the nascent HIE industry, creating barriers to interoperability not just for HIOs and providers, but for government entities as well.

The Demonstration Projects revealed that each of the consent models have both benefits and risks. The model chosen by an HIO and its participants is an individual business decision that reflects the needs and information governance processes of each organization. All of the models require tradeoffs and depend on the particular interests and needs of the affected stakeholders.[41] Stakeholders believe the barrier is the lack of a single consent solution in California; however the Demonstration Projects show that the challenges go beyond that – the foundation for the electronic movement of health information is trust. Technology standards, data sharing agreements, clear and consistent terminology, and state and federal laws that are in alignment are the real solutions.

Recommendations

The optimal environment of health information exchange is one in which patients are fully engaged in their health care and are given the opportunity to exercise choice over how their information is shared among health providers. Patients want to be reassured that their information is protected and used appropriately, but they also expect their healthcare providers to have the information when and where it is needed for treatment. Innovative technologies that create a more robust individual choice experience and provide more nuanced control over their health information – through the use of a patient preferences database, for example – will serve to support and complement existing privacy and security rules.[42]

Through the Demonstration Projects and related HIE efforts, CalOHII has identified a definitive gap. While the legal framework permits certain information to be shared without patient authorization, patients must become engaged in order for trust to be established and providing patients the opportunity to make a meaningful choice regarding the sharing of their health information is the first step for that to happen. Until technology better supports patient preferences, granular consent models, and HIO policies and processes, CalOHII makes the following recommendations. Where applicable, next steps have been identified to assist with carrying out the recommendations; however, until the industry matures, some next steps may not be fully realized.

1. **Establish a common vocabulary and change the conversation**
   In order to shift the conversation away from patient consent as a single policy lever, focus instead on the entire trust framework for sharing health information electronically. It is important to create standardized vocabulary that more accurately reflects all of the components and reduces confusion with terminology.
   - Patient preferences: previously referred to as consent or authorization. This refers to the patient's meaningful choice for sharing their health information electronically. The active process of obtaining a meaningful decision from the patient should occur regardless of the system conditions of the HIO, i.e. whether opt-in or opt-out.

[41] Goldstein, *supra* note 3, p. 28
[42] CDT, *supra* note 6, p. 22

- System conditions: The terms opt-in and opt-out should refer to the default condition of the HIE system, not the consent model chosen by the HIO. In an opt-in system, the "switches" are turned off and no patient information is shared until it is turned on; conversely, in an opt-out system, the "switches" are turned on and patient information is shared until the patient instructs otherwise.
- Governance: there are numerous types of governance; in general, governance refers to the establishment and oversight of a common set of behaviors, policies, and standards that enable trusted electronic health information exchange. Additional types of governance include:
    - Information governance – system of decision rights and accountability that encompasses the information lifecycle and information systems of an organization; may include IT management.
    - Data governance – overall management of the availability, usability, integrity, and security of the data employed in an organization or enterprise.

➢ Next Steps:
- Align California law with federal law so language is consistent.
- Provide education to HIOs, including webinars, issue briefs, and other tools to aid in understanding and implementing the trust framework.
- Assist with patient education about health information exchange, including the development of education materials, public service announcements, and website content.

2. **Continue to let the choice of system conditions (consent model) be an individual HIO business decision.**
   HIOs determine whether opt-in or opt-out system is most appropriate based on their internal governance and business processes. State and federal laws serve as the foundation, with a minimum threshold of policies and procedures providing additional layers of protection. The type of business model adopted by an HIO may dictate the policies and processes needed for obtaining meaningful choice from the patient – i.e. a federated model of exchange with a repository may require a higher level of education and permissions than a conduit model of exchange where only directed exchange for treatment purposes occurs.

   ➢ Next Steps:
   - Develop minimum standards for HIOs. These standards may be developed by state agencies, private organizations, or some combination of the two.
   - Continue to promote the use of standard agreements, i.e. the Model Modular Participant Agreement[43], and assist with the development of education materials to help patients better understand HIE.

3. **Patients must be provided an opportunity to make a meaningful choice regarding the sharing of their protected health information.**
   Because patient engagement and education is critical to helping patients understand their options for sharing their health information and the impact of those choices, active patient

[43] The Model Modular Participants Agreement is a navigation tool for health information exchange contract terms and conditions between an HIO and its Participants. The MMPA was developed under the direction of CalOHII with funds from the ARRA State Cooperative Agreement Grant. www.ohii.ca.gov

choice is mandatory for the electronic movement of health information. Patients must be provided the opportunity to make a meaningful choice regarding the sharing of their health information. Education should be offered in a variety of formats (i.e. videos, pamphlets, conversations with providers), in easy-to-understand language, with acknowledgement from the patient to further ensure interaction and engagement.

It should be noted that an organization's meaningful choice policy does not limit liability under state or federal laws; additionally, it does not limit responsibility when authorizations are required pursuant to certain state and federal laws, e.g. 42 CFR for substance abuse.

- Minimum policy requirement: Acknowledgement by the patient confirming education regarding the organization's policies and procedures (i.e. signature, electronic approval, email, etc.).
- Best practice: The ONC Tiger Team's recommendations provide a model for meaningful choice. According to the ONC, patient education and engagement should communicate that the patient's decision is:
    - Made with full transparency and education,
    - Made only after the patient has had sufficient time to review educational material,
    - Commensurate with circumstances for why health information is exchanged,
    - Not used for discriminatory purposes or as a condition for receiving medical treatment,
    - Consistent with patient expectations, and
    - Revocable at any time.

➢ Next Steps:
    - Make providers aware of tools such as sample forms and education materials.
    - Establish minimum requirements for what the meaningful choice policy should include and/or address, including minimum timeframes for obtaining patient preferences.

4. Technology solutions must evolve to support granularity of patient's meaningful choice (consent).

Patients not only prefer to be given the choice to share their health information, but they want granularity and data segregation to designate which information can be shared and with whom. Current technology does not support granular patient choice or segregation of data elements. Additionally, the paper-based process is not scalable and there is limited technology available for electronic signatures. The technology must support policy decisions, rather than drive them. The Demonstration Projects were not able to evaluate technology solutions; however, there remains a need to gather additional data and conduct testing of technology solutions that promote granular choice and data segregation, as well as electronic processes for managing patient preferences.

➢ Next Steps:
    - Convene vendors to discuss and collaborate on how technology can better support privacy and security policies.
    - Partner with the Health Information and Management Systems Society (HIMSS) on collaboration, outreach, and national standards.

- Conduct additional demonstration projects to further explore solutions to address outstanding gaps in technology and policies.

5. **Governance of interoperability is needed to sustain efforts.**
   There is a distinct difference between information governance and data governance. A strong information governance program, beginning with the State, can accelerate the goals of the Triple Aim. The Demonstration Projects helped identify the need for other governance initiatives. Legislation hasn't been enacted to govern HIE at this time, but it is clear that more work needs to be done. The industry needs to drive governance, but the State needs to provide the oversight of both information and data governance to ensure interoperability by serving as the leadership to drive strategic direction for information management.
   - Next Steps:
     - Convene and facilitate multidisciplinary steering groups to address specific priorities.
     - Conduct additional demonstration projects to further explore solutions to address outstanding gaps in technology and policies.

Appendix A: eHealth in California

Overview

A wide-scale systemic, state and nationwide infrastructure is the foundation of a modern healthcare system, with the building blocks consisting of electronic health records (EHRs) used by providers to manage patient information, personal health records for individual access to their own records, and health information exchange (HIE) to facilitate the appropriate electronic movement of information among health IT devices and systems. The federal government invested in this infrastructure with the passage of the Health Information Technology for Economic and Clinical Health (HITECH) Act in 2009, which provided tens of billions of dollars in financial incentives to physicians and hospitals for the adoption and "meaningful use" of EHRs, as well as grants to help states stimulate HIE efforts. Although HIE is still considered to be in its infancy, it has the potential to be a significant force in improving the quality, accessibility, and cost effectiveness of healthcare.

Over a decade before HITECH, the federal government recognized the need for standardization and protections for ensuring the privacy and security of individually identifiable health information. Passed by Congress in 1996, the Health Insurance Portability and Accountability Act (HIPAA) established technical standards to improve the efficiency and effectiveness of the health care delivery system by promoting widespread use of electronic data platforms and defined policies, procedures, and guidelines for the privacy and security of health data. Since then HIPAA has undergone several updates, including the adoption of current electronic transaction standards in 2009,[44] and implementation of provisions of the HITECH Act to strengthen the privacy and security protections for health information.[45]

The HITECH Act built on the early efforts of modernizing health care by promoting widespread adoption EHRs and electronic health information exchange. Benefits of meaningful use include complete and accurate information, better access to information, and patient empowerment.[46] HITECH also included updates to privacy and security provisions under HIPAA, including expanding the direct liability to business associates of covered entities,[47] which may include health information organizations, health IT service providers and those who "mine" data.

There are typically three different types of governance models of HIOs: centralized, federated (or decentralized), and hybrid.[48] The choice of architecture is driven by the organizations internal governance, as well as their privacy and security policies and procedures.

- Centralized model – patient demographics and clinical information is transmitted to a shared repository. The centralized repository is queried to obtain a patient's linked results and other information.

[44] Centers for Medicare and Medicaid Services, www.cms.gov
[45] U.S. Department of Health and Human Services, www.hhs.gov
[46] Office of National Coordinator for Health Information Technology, www.healthit.gov
[47] HIPAA Administrative Simplification standards apply to any entity that is a health care provider that conducts certain transactions in electronic form, a health care clearinghouse, or a health plan. A business associate is defined as a person or entity that performs certain functions or activities that involve the use and disclosure of protected health information on behalf of, or provides services to, a covered entity.
[48] Linda Bailey-Woods et al, "Ensuring Data Integrity in Health Information Exchange", American Health Information Management Association (AHIMA), 2012

- Federated model – the data source organization (i.e. provider) maintains custodial control over the patient's medical record. Upon request, the data is queried from the data source organization.
- Hybrid model – a mixture of federated and centralized models. The most common hybrid is one in which only some of the data is stored centrally, with other data stored in "vaults" or "edge servers" that are controlled by each organization that contributes data.

In addition, there are three key forms of HIE: directed exchange, query-based exchange, and consumer mediated exchange.[49] Directed exchange gives healthcare providers the ability to send and receive patient information over the internet via encrypted, secure and reliable messaging. This is also referred to as "push" technology. Query-response exchange – also referred to as "pull" – allows providers to find and/or request information on a patient from other providers, sometimes from a centralized repository. Consumer mediated exchange gives patients the ability to aggregate and manage their health information over the internet, sometimes referred to as a "patient portal".

While these variations in governance can be helpful, allowing each HIO to set policies and processes appropriate to the communities they serve, it also poses challenges to patients, providers, and policymakers. To help address the need for standards among HIOs, CalOHII developed the Model Modular Participants Agreement, which is a customizable model agreement between an HIO and its data providers. The MMPA outlines five increasingly complex HIO models, from Model #1, where the HIO serves as a conduit of patient information and does not have access to or maintain patient data (i.e. directed exchange), to Model #5, where the HIO operates as a federated health information exchange and aggregates and/or maintains a repository of patient data (i.e. query-response) .[50] The HIO model chosen may impact the consent policy implemented depending on whether the provider retains control over sharing patient data (e.g. Model #1) and consent for treatment, payment, and operations is not required except when otherwise required under the law (i.e. sensitive health information). However, when the decision to disclose or exchange patient data is no longer in the control of the provider, such as with a federated HIO (e.g. Model #5), then patients should be given the opportunity to make a meaningful choice about how their information is shared.

The underlying ehealth infrastructure incorporates protections for patient privacy and confidentiality. In order to achieve sustainability and ensure success, electronic exchange efforts must establish trust relationships with all participants, including patients.[51] In general, patients and consumers support the efforts of HIT and the electronic exchange of information, but they also want to be assured of the privacy and security of their health information.[52] A comprehensive policy framework based upon common principles ensures that available technology is used to improve health care, while minimizing risks and protecting health information privacy.

[49] Office of National Coordinator for Health Information Technology, www.healthit.gov
[50] MMPA Release 2.2, http://www.ohii.ca.gov
[51] Goldstein, *supra* note 3, p. 2
[52] California HealthCare Foundation, *supra* note 12, p.2

The foundation for current privacy and security policies is built upon the Markle Connecting for Health Common Framework for Private and Secure Health Information Exchange. The Markle Common Framework is based on Fair Information Practice Principles (FIPPS) and provides initial elements of a comprehensive approach for secure, authorized, and private health information sharing.[53] These principles (Figure 1) became the basis for current privacy and security policy development, including the Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information by the Office of National Coordinator (ONC) for Health Information Technology.

Figure 1 - Fair Information Practices

- Openness and transparency
- Collection limitation
- Purpose specification and minimization
- Data integrity and quality
- Use and disclosure limitation
- Individual participation and control
- Local control

California Landscape

California boasts the largest population of the 50 United States – approximately 38 million residents – and is the third largest state geographically. Approximately 80% of California is rural, yet 85% of the population lives in urban areas, creating diverse scenarios regarding access to care in both rural and urban communities.[54] This huge range of diversity creates a complicated and divided technology landscape. In this way, California is truly a microcosm of the entire United States, reflecting the diverse technology challenges seen on a national level.

In the past several years, two types of HIOs have emerged across the state: *community HIOs*, which are supported by a number of unaffiliated health care organizations, often within a geographic medical service area, and *enterprise HIOs*, which are supported by a single hospital, health system, or integrated delivery network (IDN). As of October 2013, there were 16 community HIOs identified by CalOHII as either emerging or operational, with a population target of approximately 12.8 million, and 14 enterprise HIOs with a population target of approximately 13 million. For a map that shows the most recent coverage area of community and enterprise HIOs, please see Appendix B.

Early in California's quest to make patients' health records available for medical decisions, stakeholders voiced a strong preference for a decentralized approach to HIE.[55] Because health care is local, the prevailing sentiment was that each community should be supported in developing systems and governance that best meet its particular needs. At the same time, stakeholders endorsed leveraging national and state policies, standards, and capabilities for exchange within and between HIE initiatives. This privately driven, publicly assisted model has been core to California's statewide efforts.

Whereas a majority of states created a single statewide HIE to collect and share healthcare data, California opted for a strategy that follows a neutral connectivity model: an approach in which regional community and enterprise exchanges, registries and other health information resources, and consumers connect to individual information sources as needed, supported and coordinated by a set of services that all resources share.[56] Under this model, any organization that meets a minimum set of policies, procedures and technical standards that establish a trusted exchange environment can connect and exchange information. The neutral connectivity model has the most flexibility to adapt to California's

[53] Markle Common Framework for Private and Secure Health Information Exchange, www.markle.org
[54] CalOHII, California Health Information Exchange Strategic and Operational Plans, March 2010, p. S-4
[55] CalOHII, California Health Information Exchange Strategic and Operational Plan, October 2012, p. 62
[56] *Id*., p. 21

complex healthcare ecosystem, since several regional community HIOs already exist, many large institutions have significant geographic distribution across California and have created "enterprise exchanges" to meet their needs, and public health resources are becoming electronically enabled. In addition, the neutral connectivity model emphasizes local autonomy to create and operate the services best meeting the needs of the local users, with overarching governance[57] and coordination at the state level.

Related HIE Activities

At the California HIE Stakeholder Summit in November 2012, stakeholders voiced continued frustration at the lack of guidance and requested that CalOHII "solve the consent problem." An ongoing and significant challenge is that CalOHII does not have the authority to govern HIE in California and therefore is unable to draft or enforce regulations regarding patient consent. Although the Assembly Bill 278 (Statutes of Monning, 2010) Demonstration Projects were intended to help provide needed guidance on consent, the Participants were still in the planning stages and a full assessment was not expected until late 2013.

Additionally, as part of the California HIE Strategic and Operational Plan, CalOHII aimed to increase outreach to the HIE community, including education and communication on a variety of topics and issues critical to the successful implementation of HIE in California.[58] An early finding of the Demonstration Projects indicated a clear misunderstanding of the requirements for patient authorization and consent in state and federal laws, such as HIPAA and CMIA, as well as the lack of standard definitions for the terminology used throughout the HIE community.

Pursuant to its core functions, CalOHII continued to monitor HIPAA activities among state departments and provided necessary guidance and oversight related to HIPAA implementation. HIPAA serves as the foundation to current HIE efforts, especially privacy and security of protected health information; it is critical that CalOHII continually ensure that projects and activities closely align with the statutory responsibilities of CalOHII. Concurrent with the Demonstration Projects, several other initiatives occurred that helped provide stakeholders with valuable and critical interpretations of laws as they exist today, assessments of the HIE landscape in California, and patient preferences around data sharing, including the establishment of a much-needed governance framework for trusted exchange. This section highlights some of those initiatives and their impact to and intersection with the Demonstration Projects.

Patient Authorization Project

Whether the exchange is paper-based or electronic, compliance with applicable laws is determined at the individual disclosure level. For example, an authorization from the patient allowing a behavioral health provider to disclose protected health information (PHI) to a primary care provider for purposes of treatment must be obtained whether the provider is to receive the data electronically or via paper. Under both state and federal laws, there are instances in which patient authorization must be obtained

[57] There are many types of governance when talking about health information. In this context, governance refers to the establishment and oversight of a common set of behaviors, policies, and standards that enable trusted electronic health information exchange among a set of participants, in this case organizations or entities involved in the electronic exchange of health information.
[58] CalOHII, "State of California HIE Progress Report", November 2012

before releasing a patient's PHI; likewise, there are other cases in which obtaining patient authorization is not required.

During the course of the Demonstration Projects, it became evident that not only are the state and federal laws governing health information complex, but that the terminology is not standard and there is general confusion, specifically around the terms consent and authorization. While the purpose of the Demonstration Projects was to evaluate consent, CalOHII recognized there was a critical and immediate need to help providers understand and navigate the applicable laws and regulations. Through discussions internally and with stakeholders, CalOHII explored in greater depth the understanding of the state and federal laws around consent and authorization, which lead to the development of the *eHealth Patient Authorization Guidance Tool ("Authorization Tool").*[59]

The Authorization Tool and supporting documents provide guidance on when patient authorization is needed for treatment-centered electronic health information exchange in California. The required elements of a valid authorization are set forth in the Code of Federal Regulations Title 45 Section 164.508(c)(3) and California Civil Code Sections 56.11-56.14 and 56.21. The intent is to guide providers who are exchanging health information electronically, though the rules described also apply to information in paper form. After receiving initial feedback from the industry, CalOHII is in the process of making refinements to the Authorization Tool to better outline the applicable laws and regulations and craft a revised tool for providers.

Consumer Consent Preferences Survey

In the design and implementation of new, electronic health information networks, numerous technical obstacles and ethical concerns must be addressed including patient attitudes toward sharing their information for healthcare and research. Consumers generally believe that the electronic nature of EHRs poses risks to the privacy and security of their health information but individuals are not uniform in their perspectives. Some research shows patients believe that benefits of EHRs may outweigh such risks while others report a more polarized set of opinions. Few large scale studies have been conducted on these views among U.S. consumers.

To better understand consumer preferences regarding electronic health information sharing, CalOHII contracted with University of California, San Francisco (UCSF) to perform a random-digit dial telephone survey to provide evidence of California consumers' views and preferences that can inform policymakers and the generation of patient-centered electronic health networks. The survey is part of a larger study called Scalable National Network for Effectiveness Research (SCANNER) which involves San Francisco State, University of California, San Diego, The RAND Corporation, Harvard, Vanderbilt, and Tennessee Veteran's Administration. The project was funded by the Agency for Healthcare Research and Quality with additional funding from CalOHII for the telephone survey conducted in early 2013 using computer assisted telephone interviewing (CATI) software.

The primary research questions to be answered were: 1) What are California consumers' attitudes towards sharing of health information through electronic networks (including electronic health records, distributed research networks, health information exchanges); and 2) Are there differences in attitudes

[59] CalOHII website, www.ohii.ca.gov/calohi/PrivacySecurity/ToolstoHelpYou/AuthorizationGuidanceTool.aspx

toward electronic data sharing within institutions, among closely affiliated organizations, or in large-scale networks?

Below are selected preliminary findings.[60]

- The respondents were less diverse than the California population in general with more white respondents and fewer minority respondents. The respondents were highly educated with over 75% having some college education or higher. (See Figure 2)
- A moderate percent of respondents are using the Internet to communicate about their health: 36.8% have emailed their doctor or nurse. 11.5% have used the Internet to connect to other patients for support or information, and 9.5% have participated in an online patient community such as a chat room or social networking site.
- Respondents prefer an opt-in consent model for sharing of health information for healthcare purposes. 66% selected opt-in with "break the glass"[61] access in case of emergency and 23% selected opt-in alone. Only 11% selected opt-out. (See Figure 3)
- Respondents are more likely to agree to share their health information electronically for research than for healthcare. 56.4% are likely to agree to share electronically among healthcare settings while 74.8% are likely to share for medical research[62] and 75.0% with an electronic research network.

Demographic variable	Number	Percent
Total Responses	800	
Gender		
Female	424	53.0
Male	376	47.0
Age, years, mean and range	53	18-99
Race/Ethnicity		
White (non-Hispanic)	448	56.0
Hispanic/Latino	183	22.9
Asian/Pacific Islander	64	8.0
Black	37	4.6
Mixed/Other	39	4.9
Native American	9	1.1
Education		
Up to high school	191	23.9
Some college	216	27.6
College degree or higher	384	48.0
Geography		
Urban	673	90.6

Figure 3 - Consumer HIE Consent Preferences

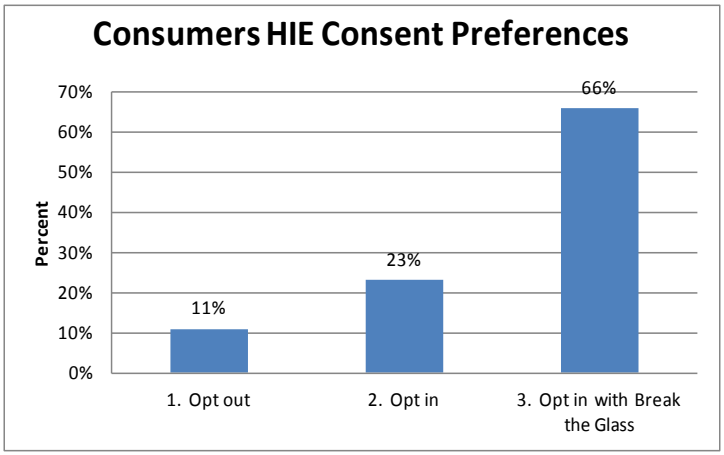

Figure 2 - Respondent Demographics

It is important to understand the variation in consumer's views and preferences with regard to privacy, security, and sharing of health information. Analyzing the survey data provides information about differences by demographic factors such as age, gender, race/ethnicity, education and urban/rural

[60] Kathy Kim 2013, unpublished data. The final research paper is expected to be published fall 2013.
[61] "Break the glass" refers to the ability of providers to access patient electronic health records in emergency situations. It is typically implemented as a firewall, whereby providers must make an attestation prior to gaining access to patient information.
[62] Research in this study refers to the use of unidentified health information for medical research studies, including large medical research studies.

location, as well as the factors that predict those views and preferences such as opinions about EHRs, quality of care, and the importance on individual control. Refer to page 12 for a discussion on how this relates to the Demonstration Project findings.

Updates to Confidentiality Medical Information Act (CMIA)

As discussed earlier in this report, California's legal protection for the confidentiality of health information is an amalgam of inconsistent provisions, piecemeal revisions, and a confusing framework of complex requirements. California healthcare entities must also comply with federal laws protecting health information, including HIPAA. While HIPAA is more comprehensive than state law, it is not above criticism. Most notably, HIPAA has no heightened protection for sensitive information, while California law provides special protection for certain types of sensitive information.

The two primary state laws on the confidentiality of health information have not been revised to reflect HIPAA or HIPAA evolution. Given the lack of consistency within California law, the lack of alignment between California law and HIPAA, and the individual nature of preemption analyses, there is no one, comprehensive "rule" for the use and disclosure of health information in California. As the health care industry begins to use electronic exchange of health information to improve efficiencies and ensure quality of care, the complexities in the law and the lack of consistent understanding of the law by health care entities is a barrier to progress. For example, many software vendors are unable to implement the capabilities needed to support granular patient permissions (i.e. for sensitive health information) because the laws and policies are too complex and stakeholders and policymakers are unable to reach consensus on what the laws allow, or recommend policies to support the electronic exchange of information.

Following the elimination of CalPSAB, the Privacy Steering Team continued to identify law harmonization as a critical issue; additionally, the California HIE Strategic and Operational Plan called for the harmonization of state law with federal rules on the privacy and security of health information.[63] In order for the State to develop a privacy and security framework to effectively support the transition to electronic health information exchange, the State must identify and address necessary changes in state privacy and security laws. The Privacy Steering Team completed a comprehensive review and recommended revisions to California law to better align CMIA with HIPAA in September 2012.

Overall, the message received was that there was recognition that the proposed work of harmonizing applicable law in California is likely to improve the privacy-preserving strengths of California law as compared to HIPAA, but that a significant amount of additional communication and discussion is required to ensure stakeholder support for recommendations. As a result of the feedback, CalOHII made a course change. Understanding the complexities and the enormity of completely rewriting CMIA, CalOHII made the decision to parse out the process and focus on making strategic updates that bring the state and federal laws into alignment, while still having a significant and positive impact to the electronic exchange of information. One critical area is to incorporate HIPAA definitions into CMIA, creating a standard set of terms around the sharing of health information. Other potential updates address the electronic exchange of health information and better reflect the current industry.

The need for privacy and security policy changes based on a comprehensive trust framework is well understood by eHealth leaders in California. CalOHII's outreach and stakeholder support efforts,

[63] CalOHII, *supra* note 56, p. O-113

including the alignment of state and federal laws, collaboration and education, and the HIE Demonstration Projects, are helping to build that trust fabric and make robust HIE a reality across California. CalOHII continues to facilitate discussions on this matter with a large spectrum of diverse stakeholders and has achieved consensus that alignment with HIPAA is urgently needed; there is consensus that the ideal solution would be a comprehensive revision of California law. The information gathered and the lessons learned through the HIE Demonstration Projects are intended to assist in these efforts.

Governance of HIE

As part of the strategic planning process after receiving the State HIE Cooperative Agreement award, CHHS performed an extensive environmental scan of the California marketplace, surveyed approaches of multiple other states to leverage the lessons learned and experience, and went to great lengths to engage California stakeholders to relate the information gathered and understand their interests and requirements.[64] Multiple governance models were considered along a continuum including a market-driven approach, a state-run governance structure with collaborative stakeholder advisory process, and a statewide governance entity with strong state participation.

Initially, it was concluded and addressed in legislation[65] that the preferred model for California was to have a not-for-profit organization serve as the HIE Governance Entity, with a diverse board and an open and transparent governance process including strong state participation to ensure achievement of public policy goals. While the HIE Governance Entity would lead the process of convening the statewide collaboration process to develop statewide HIE services, the State would play a strong role through CHHS involvement and coordinating activities.

The policies, requirements for operational procedures, and technology standards constitute governance for statewide HIE in California and establish acceptable behavior of organizations that exchange health information. Trust is the foundation for health data exchange; all parties, from patients to providers to health plans and the government, must trust each other in order for the benefits of health information exchange to be realized. The technology component of the trust environment, "Directory and Trust Services", forms a keystone of the overall exchange strategy and architecture.[66] Although CHHS does not have statutory authority to govern HIE in California, it was identified that the agency would play a critical role in facilitating the development of governance for HIE by bringing together industry leaders with proven ability in advancing HIE. Thus, CalOHII convened several established organizations already engaged in several initiatives, including the Demonstration Projects and Directory and Trust Services.

In February 2013, CalOHII held an information gathering session to identify the need for governance and what organizations might be involved. Industry leaders from community and enterprise health information organizations were identified and invited to attend an all-day brainstorming meeting held to discuss the need for HIE governance and the need for establishing trust and facilitation of exchange among unaffiliated organizations in California. During the meeting, the stakeholders agreed that there was a need to establish an organization that would promote interoperability among healthcare providers and create a trust framework based on national standards and protocols for trusted exchange. In addition, it was important to create pathways to ensure that all providers can connect to and use

[64] CalOHII, *supra* note 56, p. S-18
[65] California Health Information Technology Act, Health and Safety Code § 130250
[66] CalOHII, *supra* note 57, p. 27

existing nationally-developed architectures for inter-HIO data sharing – the Direct Project and eHealth Exchange.

After several additional meetings, the group formally established itself as the California Association of Health Information Exchanges (CAHIE), a statewide group of community and enterprise health information organization leaders working together to advance safe and secure HIE throughout California. CAHIE's mission is to establish a self-governance function for trusted exchange in California, relying on the National Coordinating Committee for national governance, but filling gaps with those additional functions California members require to achieve a trusted exchange relationship with each other. Immediate goals include the development of a comprehensive California addendum to the federal Data Use and Reciprocal Support Agreement (DURSA) that calls out refinements and clarifications of policies and procedures relative to HIE in California; development of a multi-party trust agreement allowing parties to interoperate using the national standards for Direct and Exchange; and establishment of policies and procedures for the California trust network.[67]

In general, governance refers to the establishment and oversight of a common set of behaviors, policies, and standards that enable trusted electronic health information exchange among participants. There is growing focus on *information* governance as a driver of the health information transformation. Information governance involves the accountability framework and decision rights to achieve enterprise information management (EIM), which is the infrastructure, policies, and procedures that ensure information is trustworthy across the organization.[68] With information no longer in silos, healthcare EIM must span the life cycle of information and bridge organizations and systems, as well as engage and support the needs of patients, families, and communities in which they live.[69] Effective information governance enables all levels of healthcare professionals and engenders trust in the data. While the principles of information governance and enterprise information management typically relate to healthcare organizations, the state can serve as the key driver of the guiding principles that provide a stable navigation system.

[67] CalOHII website www.ohii.ca.gov/calohi/PrivacySecurity/CAHIE
[68] Linda L. Kloss, "Leading Innovation in Enterprise Information Governance", *Journal of AHIMA*, September 2013, pp. 34-38
[69] *Id*., p. 37

Appendix B: Current HIO Landscape

Community Health Information Organizations (HIOs) in California

OCTOBER 2013 SNAPSHOT

EMERGING

1. ConnectHealthcare
2. HealthShare Bay Area
3. LANES
4. Marin County
5. North State Health Connect
6. San Luis Obispo Medical Education and Research Foundation
7. SacValley MedShare
8. Tulare Kings Fresno Madera HIE

OPERATIONAL

- A Inland Empire HIE (IEHIE)
- B NCHIN
- C OCPRHIO
- D RAIN Central Coast HIE
- E Redwood MedNet
- F Santa Cruz HIE (SCHIE)
- G San Diego Regional HIE
- H San Joaquin Community HIE

NOTES

Icons represent HIOs providing or planning services in that county. HIOs may include many health care delivery organizations in the county or only a select group. Placement of icon does not indicate the exact geographic location of the HIO.

Shading indicates a presence but not necessarily full coverage in a county.

A Enterprise HIE services provided to health care delivery organization(s) within indicated county.

DEFINITIONS

COMMUNITY HIOs: HIOs that organize and govern HIE for a specific set of unaffiliated health care delivery organization participants, often within a geographic medical service area, to enable interoperability and secure electronic sharing of patient health information.

OPERATIONAL:* These HIOs are transmitting data between participating health care delivery organizations.

EMERGING:* Not yet transmitting data. HIOs may be getting organized, defining shared visions, goals, and objectives, identifying funding sources and technology vendors, and setting up legal and governance structures.

*Definitions adapted from the eHealth Initiative (eHI) health information exchange (HIE) maturity schema.

UCDAVIS
INSTITUTE FOR POPULATION HEALTH IMPROVEMENT
California Health eQuality

Appendix C: Demonstration Project Participant – San Diego Regional Health Information Exchange

Overview

The San Diego Regional Health Information Exchange was formed in 2011 as the San Diego Beacon Community, one of 17 communities nationwide chosen by the Office of National Coordinator for Health Information Technology as part of the Beacon Community Cooperative Agreement Program. The Beacon Program supported these communities to build and strengthen their health information technology (health IT) infrastructure and exchange capabilities to improve care coordination, increase the quality of care, and slow the growth of health care spending.

The San Diego Beacon Community (SDBC) received a three-year, $15.3 million grant from the ONC to advance the existing health IT infrastructure and HIE in the region. The goal of SDBC is to foster data exchange, interoperability, and clinical integration for meaningful use among hospitals, clinics, providers, and patients to improve the overall health of the community. The collaborative includes the only academic medical school in the region (UC San Diego Health System), two large health systems in San Diego County (Scripps Health and Sharp Healthcare), the only pediatric hospital (Rady Children's Hospital of San Diego), the VA Medical Center, Naval Medical Center, and all Federally Qualified Health Center clinics in the San Diego community. Additional partners include the County Public Health Department, San Diego City Emergency Medical Services agency, California Institute for Telecommunications and Information Technology, and San Diego State School of Public Health.

The San Diego Beacon Community clinical goals include:

- Improve the care of heart attack victims by linking prehospital care to the community HIE and sharing individual health information from the prehospital field setting, including electrocardiograms, with hospital providers electronically;
- Improve rates of immunization and reporting by linking the community HIE to an existing immunization registry;
- Reduce rates of 30-day hospital readmissions by improving quality of care and care coordination between providers with access to individual health information through the community HIE; and
- Reduce rates of unnecessary and repeat complex radiology studies (computed tomography and magnetic resonance imaging) by improving provider access to recent studies through the community HIE.

The SDBC community HIE allows authorized providers to request and access a complete and up-to-date medical record from other participating providers who have also seen the patient for clinical care. The HIE launched in December 2011 starting with pilot sites at Children's Primary Care Medical Group, Rady Children's Hospital, UC San Diego Health System, and VA San Diego Healthcare System. Kaiser Permanente Southern California began exchanging data with the San Diego Beacon Health Information Exchange in November 2012.

In 2013, the San Diego Regional Health Information Exchange (SDRHIE) was created as an independent, community organization with the mission of improving the health of all San Diegans through advances in health IT. The new organization assumed leadership and oversight of the San Diego Beacon

Community, including oversight of the community HIE. Services of the HIE include real-time transmission of electrocardiograms and patient information from ambulances to hospital emergency departments; and electronic reporting of immunizations and infectious diseases to County public health to improve public health surveillance and prevention.

Consent Demonstration Project

The SDBC Privacy and Liability Workgroup focuses on reviewing, developing, and implementing best practices for HIE privacy and security issues in coordination with state and federal laws. Under the guidance of the Workgroup, SDBC made the business decision to implement an opt-in consent model for the HIE, with patients given the opportunity to select one of three options: emergency (only allow access in the event of an emergency), full (access information for all health care encounters), or none (do not allow access). The Privacy and Liability Workgroup worked with the CalOHII Privacy Steering Team on the creation of an opt-in consent form and patient educational sheet.

San Diego Beacon applied to be a Participant in the Demonstration Projects in 2011 and a signed Memorandum of Understanding was completed in February 2012, following the implementation of the Demonstration Projects regulations and the launch of the SDBC HIE. The initial participating organization of the Demonstration Project was UC San Diego Health System, with one clinic to pilot the consent form and process. At that time, the patient's consent status was not stored centrally in the HIE and each participating organization of the HIE managed the consent process separately. From the time of the original application and the actual start up of the pre-planning work of the Demonstration Projects, additional participating organizations were signing on with the Beacon HIE and the MOU was revised to allow a hybrid consent model to be tested, in accordance with the Demonstration Projects regulations. This would allow organizations with an opt-out consent process (e.g. Kaiser Permanente) to be included in the Demonstration Projects.

The Demonstration Project evaluation was scheduled to begin in September 2012, but technical delays resulted in the evaluation beginning in December 2012. After an initial outreach by the VA San Diego Health System, resulting in 700 patients consenting to share their health information through the exchange, an additional 200 patients went through the consent process during the initial evaluation phase. As of March 2013, approximately 944 patients had been through the consent process, with 894 agreeing to share data completely and 25 for emergencies only.[70] Rady Children's Hospital was consenting patients, but the consent status was not being transmitted electronically to the HIE. A new MOU was created with SDRHIE to include Rady Children's Hospital as a Demonstration Project Participant and a new evaluation period began in April 2013.

Rady Children's Hospital submitted monthly data to CalOHII through September 2013. The process for capturing consent is included with the hospital registration process – the registration staff presents the informed consent form to every patient until the patient has either made a choice or requests not to be asked. Rady Children's Hospital began the consent process in July 2012 and saw a 95% opt-in rate in the nine months leading up to the start of the Demonstration Project; that opt-in rate remained constant through the evaluation period and by the end of the Project nearly 93% of active patients had been through the consent process. Rady Children's Hospital attributes their high rate of success to a streamlined process that did not add additional administrative burden, as well as a having executive leadership that strongly believes in the value of health information exchange. Because Rady Children's

[70] Combination of VA patients and patients at one clinic within UC San Diego Health System.

Hospital provides care to approximately 80-90% of the children in the San Diego area, there is a large incentive to participate in health information exchange activities.

By the end of the Demonstration Project, Rady Children's Hospital was submitting consent status information to the HIE via electronic messages to be stored in the master patient index. All of the participating organizations that use Epic as their EHR technology vendor (RCH and UCSD) will transmit consent electronically to be stored centrally in the HIE; all other participating organizations will manage consent status locally and will not submit consent status to the HIE. UCSD was scheduled to begin the informed consent process in September 2013.

Data

	Opt-In Rate	Total Authorized	Total Denied	Total Emergency Only	Total Patients
Rady Children's Hospital	95%	192,748	10,039	5,388	208,175
UC San Diego	97%	894	25	25	944

Notes:

1. Authorized means affirmative consent to share health information.
2. Denied means explicit denial to opt-in to sharing health information. Total patients denied also include unsigned consent forms and foster parents who are not authorized to sign the consent form.

Appendix D: Demonstration Project Participant – Inland Empire Health Information Exchange

Overview

Developed in 2009, the Inland Empire Health Information Exchange (IEHIE) is a collaborative of Riverside, San Bernardino and other California County hospitals, medical centers, medical groups, clinics, IPAs, physician practices, health plans, public health and other healthcare providers. IEHIE brings needed technology to access and securely share electronic patient health records for more than 5 million people living in Inland Empire and other communities. The population represents a diverse culture with Hispanics representing more than 45% of the population including a high rate of Medi-Cal beneficiaries. The Inland Empire is challenged with poor patient access due to low very low provider to population ratios and with very poor health ratings within the state.

IEHIE contracted with Orion Health Inc. to coordinate the community based HIE. IEHIE's vision revolves around a secure, collaborative interoperable community environment where all of the participants in the delivery of healthcare are visible. In addition to each participant being able to make a contribution to the HIE, each participant recognizes benefit. IEHIE is addressing electronic health information exchange issues and adopted the following goals and results:

- Provide "connector" technology to share patient health information among providers
- Prioritize information sharing to ensure value creation
- Enhance clinical care transitions within the counties
- Assist participants in achieving Meaningful Use
- Provide value-based data sharing for efficiency and cost reduction
- Support new models of care, such as Accountable Care Organizations (ACOs)

IEHIE is one of the largest HIE's in the country and has successfully achieved financial self-sustainability through the implementation of a fee structure for members based on the membership level, organization type, and services provided.

Consent Demonstration Project

The development of the usage and consent policy within IEHIE was the product of a detailed process that included participation from the IEHIE governing body within the scope of the IEHIE Policy Committee. Detailed legal review of the policies to ensure conformance with applicable state and federal laws was accomplished and final board approval of the policies was obtained in March 2012. The policy document was developed using existing policies from other HIE settings adapted to the specific scope of the IEHIE environment incorporating input from the IEHIE coalition of members and the leadership group.

The IEHIE adopted an opt-out consent model, which was tested during the Demonstration Projects. Data is automatically shared through the HIE and patients are notified via the Notice of Privacy Practices by the provider or health plan and given the ability to opt out of sharing their health information. IEHIE is an all-in or all-out exchange, meaning there is no granularity in data sharing. IEHIE previously established and vetted the consent process with the IEHIE governing body; therefore the pre-planning work to be done was minimal. The Demonstration Project evaluation was scheduled to begin January 1, 2013, with 5 organizations agreeing to participate; however, only one site was ready to implement the

consent process and minimal data was obtained. The remaining four sites went live with the exchange in May of 2013 and the evaluation period was extended through September.

During the course of the evaluation period, three sites actively notified patients of their option to opt-out of the HIE. Inland Empire Health Plan sent notices in the mail to enrolled patients; Pacific Alliance Medical Center and Arrowhead Regional Medical Center included the IEHIE Notice of Privacy Practices in their admission packets. Riverside Physicians Network was still in the testing phase with IEHIE and had not finalized the process of opt-out notification to members. Beaver Medical Group confirmed they had not begun the process of registering patients with the HIE and were waiting until other sites were actively using the HIE to exchange data before they started the notification process. Because IEHIE is an opt-out model, all sites were actively submitting patient data into the HIE, with the exception of Riverside Physicians Network.

Data

	Opt-Out Rate	Patients Offered Choice[1]	Patients in HIE[2]
Pacific Alliance Medical Center (PAMC)	0%	985	298,937
Inland Empire Health Plan (IEHP)	0%	108,376	804,497
Arrowhead Regional Medical Center (ARMC)	0%	158,031	243,919
Beaver Medical Group (Beaver)	N/A	N/A	474,594
Riverside Physicians Network (RPN)	N/A	N/A	N/A
Total all sites	0%	267,392	1,821,947

Notes:

1. Total patients seen/offered choice is an estimate based on total encounters. Specific schedule information is not available.
2. Total patients in the HIE of organizations participating in the Demonstration Project.

Appendix E: Demonstration Project Participant – Santa Cruz Health Information Exchange

Overview

As one of the oldest and most advanced multi-stakeholder exchanges in the country, Santa Cruz Health Information Exchange (SCHIE) connects a diverse set of healthcare organizations, such as large IPAs, hospitals, clinics, national and local reference labs, imaging centers, and physician practices, and serves a broad range of providers, including primary care physicians, specialists, hospitalists, emergency room doctors, and other licensed health professionals. The HIE facilitates the exchange of a wide range of health information among participating organizations and providers, including lab results, electronic prescriptions, refill requests, pre-treatment authorizations, orders, referrals, consult letters, and radiology reports. Authorized providers in the HIE can access comprehensive patient records through the virtual health record (VHR) and electronic medical record (EMR) systems that support eHealth Exchange (formerly NwHIN) protocol and can query for patient information using Integrating the Healthcare Enterprise (IHE) web services transactions.

The mission of SCHIE is to:

- Improve the quality and efficiency of healthcare for all stakeholders in the Santa Cruz community;
- Deliver technology assistance, guidance and information on best practices to providers with the goal of creating a healthcare delivery system that offers a seamless, integrated experience for patients and providers;
- Provide services and tools to participating healthcare providers to become meaningful users of EHRs connected to the Santa Cruz HIE.

These are foundational for Accountable Care, Clinical Integration, Medical Home Model, and surviving payment reform as independent physicians.

Consent Demonstration Project

Santa Cruz HIE proposed and tested through the Demonstration Project an opt-out consent policy with an emergency exception. Patients have three consent choices:

- Yes – patient allows sharing of their health information and authorized providers may access the information for treatment purposes.
- No – patient opts out of sharing information and providers are not able to access the patient's information.
- Emergency only – patient opts out of sharing their health information except in the event of an emergency and only providers with "break-the-glass" privilege are able to access the patient's information after attesting to the emergency situation that necessitates the access.

In the absence of an explicit consent registered by the patient, consent is assumed and authorized providers are permitted to access health information in the exchange for treatment purposes. In addition to the consent policy, safeguard of patient privacy and health information is achieved by leveraging existing HIE privacy and security protections relating to authentication, authorization, access controls, and auditing.

SCHIE collaborated with CalOHII on the development of the consent form and opt-out educational material. Unlike other traditional opt-out models, SCHIE implemented a consent verification process in order to measure the implementation of the consent policy with the five participating sites. With traditional opt-out models, patient information is shared until a patient makes the explicit choice to opt out. By implementing a verification process in which they educated patients during each clinical encounter and presented patients with the choice, the consent model is more reflective of an opt-in model. However, patients that did not register a consent choice were still set to the default, which is to share their data through the exchange. CalOHII was supportive of this mixed consent process because it allowed evaluation of the effectiveness of implementing a consent process, provider engagement, and overall satisfaction with the consent policy.

The SCHIE Demonstration Project evaluation period began March 1, 2013, with one participating site; the remaining four sites implemented the consent process at various times through April 2013; data collection continued through August 2013. Patients were offered a consent form at the point of registration; additionally, patients had an opportunity to discuss with office staff and/or their physician about consent and their electronic health record in the HIE. The participating providers for this demonstration project had varied methods for updating consent status in the HIE. Consent forms were either faxed to a fax server at the HIE, picked-up at the practices by HIE staff, scanned into the HIE by the practice, or a combination of these methods.

The actual data collection process was manual, from the point of collecting the consent form from the patient to entering the data into the HIE, as well as storing and maintaining the data. The infrastructure and level of technology varied among participating providers; not all providers use their EHR's in the same manner or use all available functionality. These differences presented challenges when running analytic reports.

SCHIE processed 528,754 patient consents during the demonstration project and the current rate of opt-out is less than one-half of a percent (0.5%). Physicians reported that most patients were very comfortable with their PHI being shared amongst their treating physicians. Because of the gained trust throughout the community, providers, and patients are aware of the benefits of the HIE and patients are generally not questioning access, and prefer to continue "as is" not having to sign additional forms.

Data

	Total patients notified	Total patients seen	Average rate of consent
Site #1 – Primary Care	447	4,799	9%
Site #2 - Specialist	114	1,219	9%
Site #3 – Primary Care	2,654	5,814	46%
Site #4 – Primary Care	829	1,568	53%
Site #5 – Primary Care	591	1,051	56%
Total all sites	**4,643**	**14,451**	**35%**

Consent Status in Virtual Health Record	
Yes (“Y”)	4,981
No (“No”)	6
Emergency Only (“E”)	36
Total	**5,023**
Total Patients in VHR	**528,754**
Opt-Out Rate	**0.1%**

Notes:

1. Due to differences in how the data was collected, as well as patient matching in the master patient index, the total patients with a consent status changed during the Demonstration Project and the total patients notified/offered the choice are slightly difference.
2. The average rate of consent refers to the number of patients seen versus the actual number of patients who signed a consent form.

Appendix F: Demonstration Project Reporting Requirements

Introduction

The purpose of this document is to outline the objectives of the Demonstration Projects, what will be tested during the course of the Demonstration Projects, and how we will measure what is being tested. While the development of the criteria is a collaborative effort between stakeholders, CalOHII intends to approach each Demonstration Project in a similar manner for consistency and data validity. Issues, risks, or barriers related to collecting the necessary data will be tracked and managed appropriately.

Objectives

Pursuant to AB278, the purpose of the Demonstration Projects is to test potential privacy and security policies for the safe and secure exchange of health information, including, but not limited to, issues related to access to, and storage of, individual health information.

Through the consent Demonstration Projects we want to measure and identify specific implementation issues pertaining to patient consent for the electronic exchange of their health information. The goal is that using a number of questions related to the consent policy and the implementation of such policy by health care providers, we will find answers and gather reliable data on the policy and its effect on patients and providers.

Specifically, we will be measuring:

- The patient opt-in/opt-out rate
- Why a patient chose to not to opt-in or to opt-out[71]
- Patient satisfaction with the consent process and the education provided
- Provider satisfaction or engagement with the consent policy and processes

Definitions

For the purposes of the Demonstration Projects, the following definitions apply:

- Opt in – Default is that no patient health information is included; patients must actively express consent to be included, but if they do so then their information must be all in or all out
- Opt in for emergencies only – Default is that no patient health information is made available but the patient may allow their information to be shared in an emergency situation only ("break the glass")
- Opt out – Default is for health information of patients to be included automatically, but the patient can opt out of sharing completely
- Opt out with emergency exception – Default is for health information of patients to be included, but the patient can opt out completely except in an emergency situation ("break the glass")
- Active choice – Patient was seen in a clinical setting at a participant site during the test period and, having been offered the consent form and informing material, made the choice to participate or not in the HIE

[71] CalOHII created patient surveys to be distributed to patients who chose not to participate in the HIE, but there were no surveys returned by patients during the Demonstration Projects.

- Opt in/Opt out rate – For the purposes of the Demonstration Projects, the opt in and opt out rate will be calculated as:

  Opt in = Total # of patients opting in* ÷ Total # patients given active choice
  *Includes patients opting in completely and for emergencies only

  Opt out = Total # of patients opted out ÷ Total # of patients given active choice

Metrics

On a monthly basis, the following data will be collected from the Demonstration Project Participant.

Quantitative Analysis
Number of patients opting in/out, by category (if available): • Opt-in/out completely • Opt-in/out for emergencies only • Consent not obtained
Total unique patients offered choice
Total unique patients seen
Total patients in the Health Information Exchange
Changes in consent status: • How many patients who originally did not opt-in chose to opt-in on a subsequent visit? • How many patients who originally opted in revoked their consent on a subsequent visit? • How many patients opted out at a later visit after initially choosing not to opt out?
How many providers are not offering consent? E.g. zero opt-out rate but data is being exchanged.
What transactions were exchanged? e.g., number of HL7 messages per month, number of patient records accessed per month?
What types of data were exchanged?
How many patient complaints were there?
How many occurrences of unauthorized access were there?
How many unsuccessful attempts to access data were there, i.e. providers attempted to access data through the exchange but the patient had opted out?

Patient Survey
How many patients found the consent process helpful to understanding how their information would be shared?
How many patients want to be asked their preference for sharing data at each visit? Once?
How many patients would rather have information available to their doctor without consenting?
How many patients want the choice to opt-in/opt-out?
How many patients chose not to opt-in/opted out because (measure each): • Needed more information or time to decide • Did not understand the health information exchange • Only want information shared in emergencies • Fear information would be shared inappropriately or do not trust the security of the system

Provider Survey/Direct observation
What is the providers preferred method of educating patients (measure each): • Consent form with written material • Provider staff explanation and associated written material • Video clips • Website
How long did the consent process take?
How often did the consent process negatively impact another part of the check-in process?
How many patients had questions after the consent process?
What staff is responsible for consent process and/or education?
How many patients found the process confusing?
How many patients changed their mind after meeting with the provider?
What communication barriers impair the provider and/or staff's ability to have the patient understand sharing health information (measure each): • Language barriers • Concept of health information exchange is too complex for most patients • Educational materials in other languages are not sufficient to explain health information exchanges
How many providers had issues caring for a patient who did not opt-in/opted out?