Medical Data Sharing:
Establishing Trust in Health Information Exchange

GIAC (GLEG) Gold Certification

Author: Barbara Filkins, filkins@impulse.net
Advisor: Benjamin Wright

Accepted: 2017-03-01

Template Version September 2014

Abstract

Health information exchange (HIE) “allows doctors, nurses, pharmacists, other health care providers and patients to appropriately access and securely share a patient’s vital medical information electronically—improving the speed, quality, safety and cost of patient care” (HealthIT.gov, 2014). The greatest gain in the use of HIE is the ability to achieve interoperability across providers that, except for the care of a given patient, are unrelated. But, by its very nature, HIE also raises concern around the protection and integrity of shared, sensitive data. Trust is a major barrier to interoperability.

Legal agreements, supported by policies and procedures, are a cornerstone in developing a trust framework for HIE. Development of such a framework is challenging. This paper attempts to define some of these challenges that health information organizations (HIOs) face in establishing trust for health information exchange from the legal and contractual aspects. An actual use case will highlight some of the more critical issues, presenting the reader faced with the challenge of sharing sensitive medical data with possible solutions that he or she can use beyond the confines of this case study.

Note: The intended audience for this paper is assumed to have some basic familiarity with HIPAA and implementing regulations at Title 45 Code of Federal Regulations, although the reader may not be familiar with the concepts behind health information exchange. Readers should be aware that this paper provides a list of robust references regarding this topic as well as an appendix of acronyms.

1. Introduction

Currently, the media is fraught with headlines that yet another substantial breach of healthcare data has occurred. Few realize how dependent the health care industry is on the daily, secure electronic exchange of confidential information: health-related financial data, patient-created wellness data, patient summary information among caregivers and other authorized parties for treatment, aggregated information for population health analysis and management, and support of initiatives like precision medicine.

Interoperability is "the ability of different information technology systems and software applications to communicate [foundational], exchange data [structural or syntactic], and use [semantic] the information that has been exchanged" (HIMSS, 2013). It remains a leading focus for the healthcare industry, motivated by both Federal and vendor initiatives (McCarthy, 2017). Health information exchange presents a solution to achieving interoperability across a heterogeneous landscape of platforms and processes. Its ultimate purpose is to facilitate the secure electronic exchange of clinical information among unaffiliated healthcare entities, "allow[ing] doctors, nurses, pharmacists, other health care providers and patients to appropriately access and securely share a patient's vital medical information electronically—improving the speed, quality, safety and cost of patient care" (HealthIT.gov, 2014).

Bringing together sensitive data from disparate sources requires organizations to establish exchange mechanisms that are not just secure, but trusted as to the identity of the trading partners as well as to the integrity and quality of the exchanged data. In other words, trust is about making sure patient data is reliable and does not leak to the wrong people.

For health information exchange, specifically, establishing both trust and interoperability among two or more organizations that want to share data represents a significant barrier (Information Sharing Environment, n.d.). A trust framework ensures the data privacy and security: its integrity (encompassing quality and accuracy), confidentiality (in light of the privacy laws safeguarding PII and ePHI), and availability (including completeness of the record) (Forum, 2013).

Even for a smaller data-sharing network, both the establishment and maintenance of a trust framework among its members can be challenging. A HIE network must protect the privacy and security of data gathered from multiple sources, including disparate electronic health record (EHR) systems. Its regulatory environment must address both Federal (e.g., HIPAA) and local law. Policies and procedures must be harmonized across a variety of participants. Confusion around the relationship requiring business associate agreements (BAA) generates contractual and legal complications. Since the implementation of such a framework relies on the synthesis of multiple avenues of information, these challenges are ever-present.

The implementation of a trust framework becomes especially challenging when an independent health information exchange wishes to participate with other similar data sharing networks at an enterprise or national level. Examples of these broader trust framework serve as templates. The eHealth Exchange network and the Care Equality Trust Framework, both initiatives of the Sequoia Project, represent national effort in the United States (The Sequoia Project, n.d.). State-level initiatives also serve as models (Dierker, 2008). Other examples include enterprise (HIMSS FY16 HIE in Practice Task Force, 2016), payer-based (CalINDEX, 2016), and regional instances (San Diego Health Connect, n.d.).

Agreements and policies are needed to resolve the maze of trust issues both at the intra- and inter-network levels. This paper identifies several associated challenges and presents considerations and recommendations for their resolution, utilizing an actual use case for confirmation. The results provide inputs to a roadmap that can help healthcare organizations, not just those directly involved in HIE, navigate through establishing a trustworthy sharing of health-related data using HIE concepts.

2. Understanding the HIE Landscape

Several key concepts are needed to approach the development of a trust framework for HIE. The first is the infrastructure that ties together data requestors and data providers. Figure 1 shows a cloud-based infrastructure that illustrates the three views that a trust framework for an individual HIE network must link together.

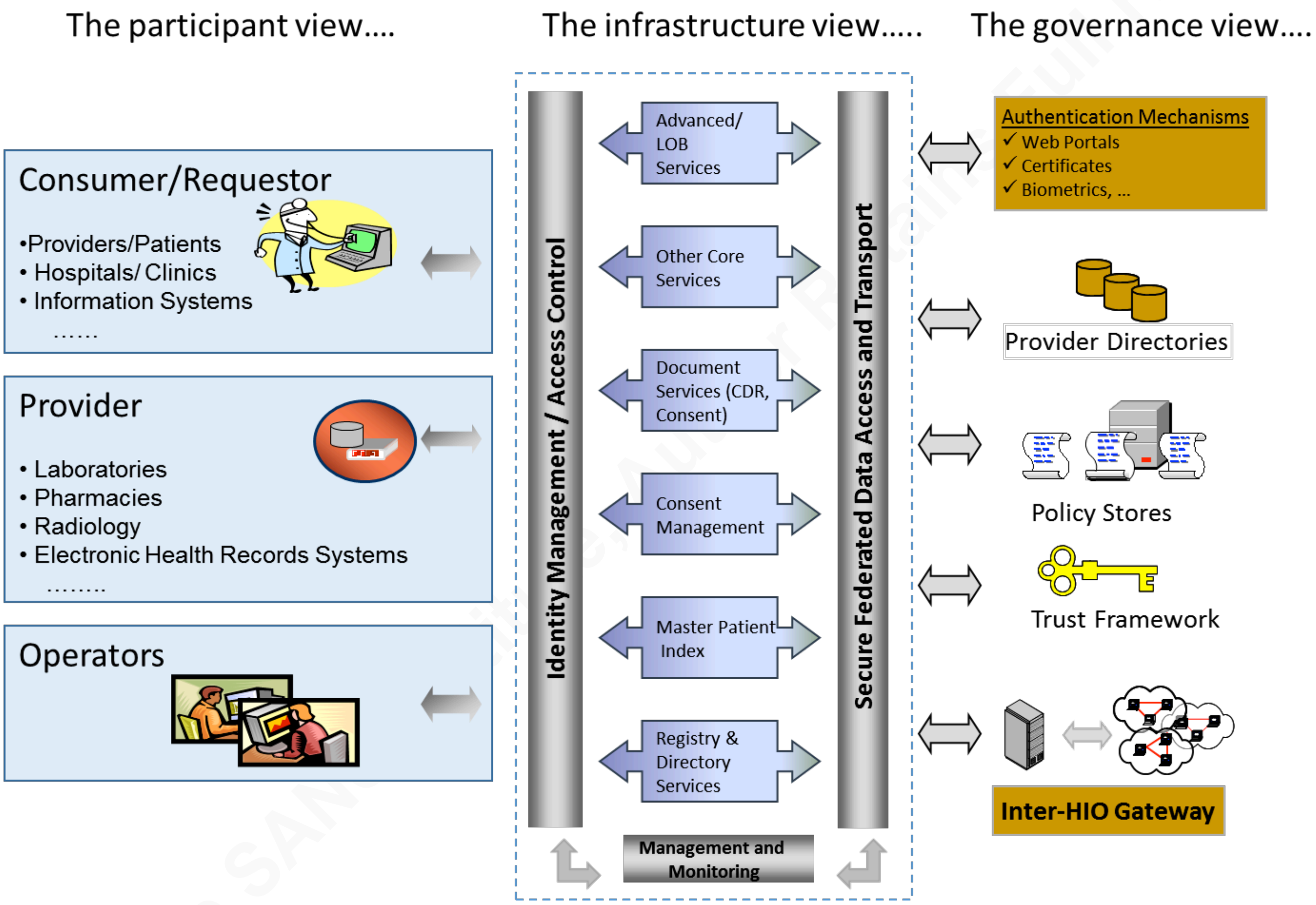

Figure 1: HIE Reference Architecture (Adopted from Filkins, 2012)

The infrastructure must provide seamless and trusted exchange of sensitive data between participants with identity management, access, and monitoring controls. It must also help to strengthen governance across a federated network by harmonizing authentication mechanisms, directory systems, and network-based policy.

The second concept to understand in the development of a trust framework is **health information organization** (HIO), the entity responsible for "oversee[ing] and govern[ing] the exchange of health-related information among organizations according to nationally recognized standards" (The National Alliance for Health Information Technology, 2008). HIOs have been forming since the mid-1990s at the local, state, and national levels, representing both the private and public sectors, within the United States and its territories.

An HIO can be considered to represent the data-sharing network of those entities which are its members or Participants. These Participants have agreed to exchange PHI through a localized trust framework unique to that HIE. In general, Participants include either covered entities or business associates of covered entities as defined by 45 CFR §160.103.[1] The HIO both manages a variety of health data sources and performs a broad range of value-added services through the HIE infrastructure that reflects the needs of its Participants as shown in Figure 2.

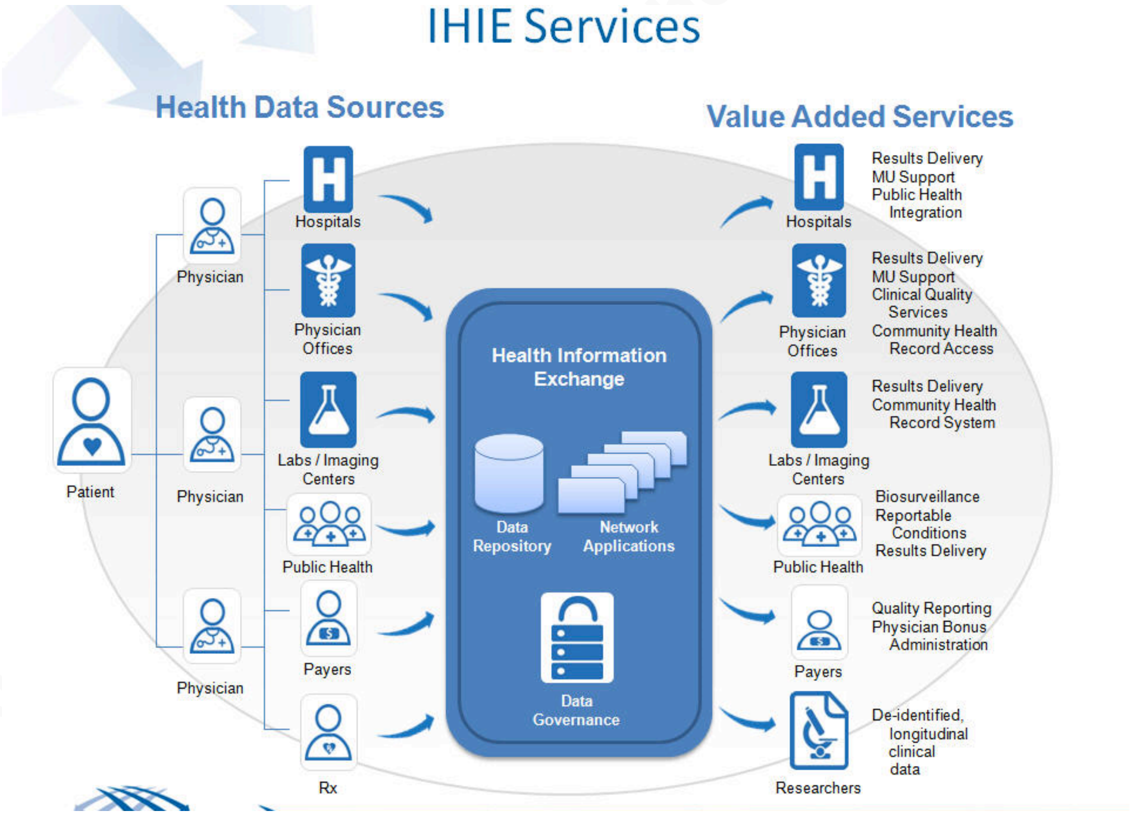

Figure 2: The Value of Health Information Exchange (Source: www.ohie.org)

Finally, HIOs can join in larger networks, such as the eHealth Exchange, forming a “network of networks” for the data exchange. At this level, HIOs are considered to “facilitate” the data exchange across the participants in each respective network, leading to complexities in defining and implementing relationships at the inter-HIO level.

[1] For the purposes of this paper, the term “HIPAA” includes The Health Information Technology for Economic and Clinical Health Act (“HITECH Act”), any other amendments to HIPAA, and all regulations under HIPAA.

3. A Framework for Trust

As entities look to exchange protected health information (PHI) in a trustworthy way, they logically avail themselves of written agreements to set standards of performance and accountability. According to David Kibbe, of DirectTrust, "a Trust Framework for Health Information Exchange is a set of technical, business, and legal standards, expressed as policies and best practice recommendations, that members of a trust community agree to follow, uphold, and enforce" (Klepper, 2013). This section explores the key artifacts that legally define, guide and enforce the relationships among data-sharing entities.

Figure 3 shows the generally accepted levels in an end-to-end HIE trust framework, based on a model that first emerged at the national level (Nationwide Health Information Exchange (HIE) Resources, 2013). [2]

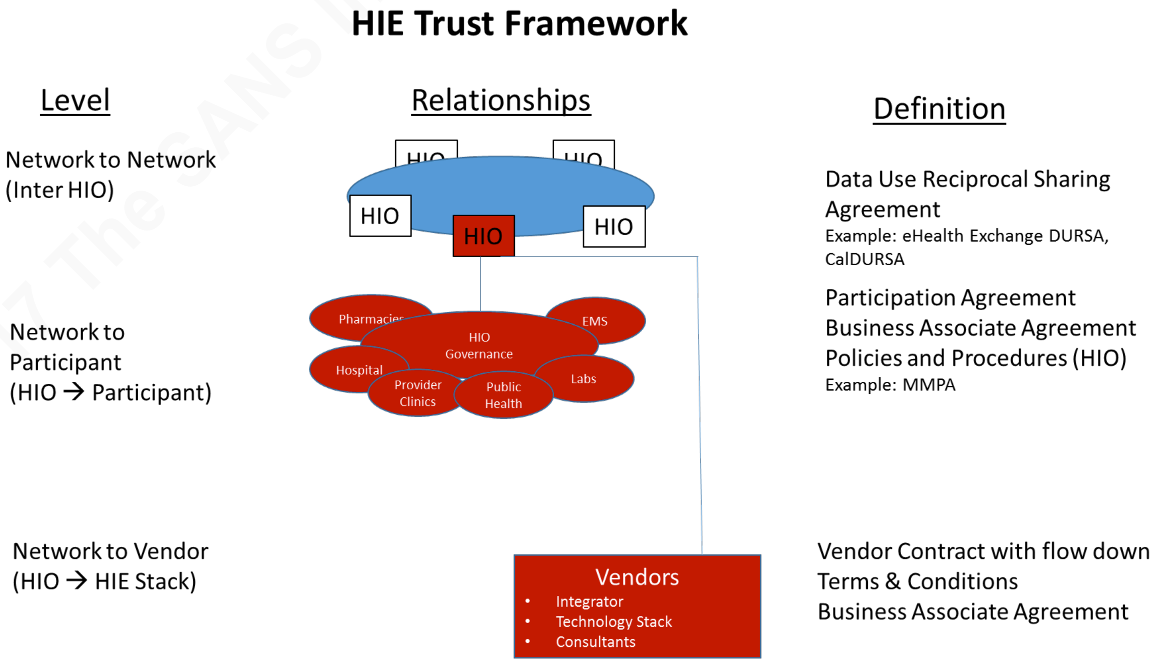

Figure 3: Layers of Trust for HIE

This model presents three major levels of trust: 1) network-to-network that establishes bilateral agreements between otherwise unaffiliated networks, 2) network-to-Participant that outlines the relationships between data providers and

[2] California is the location for the implementation scenario outlined in this paper. HIE in California follows the national model, so the model in Figure 4 will be the one explored in the use case later in this paper.

requestors sharing a common interest, and 3) network-to-vendor, where the HIO develops contractual relationships with its providers.

3.1. Data Use and Reciprocal Sharing Agreement

Mutual data-sharing agreements should be based on agreed-upon standards that encompass data governance, access, privacy, security, and intended use among other issues. As the number of health information exchanges has grown, so has the need to connect individual data-sharing networks at a network-to-network level. This, in turn, requires the need to streamline inter-HIO agreements around trust and exchange, eliminating the need for "point to point" agreements that become increasingly difficult, costly, and inefficient to maintain as participation in the "network of networks" grows.

A **data use and reciprocal sharing agreement** **(DURSA)** is commonly used to facilitate the bilateral exchange of data between individual HIO/HIE networks. "Data disclosers are expected to make data-sharing decisions based on their own organization's policies, consistent with minimum necessary legal requirements (45 CFR 164.502(b), 164.514(d))" (AHIMA/HIMSS HIE Privacy & Security Joint Work Group, 2011). Without a DURSA, a data requester on one network may logically be denied access to a data provider on another network because that data provider's (aka discloser's) authentication level or minimum data policy has established requirements that differ significantly from those of the data trading partner. The eHealth Exchange DURSA, representing national inter-HIO agreement, serves as an important model for establishing trust frameworks between independent HIE networks in compliance with applicable law (The Sequoia Project, n.d.).

3.2. Participation Agreements

The DURSA assumes that each participating HIO has an established trust relationship with its participants as defined by existing end user trust or participation agreements, policies and procedures, and vendor agreements for that specific network.

A **participation agreement** defines the relationship between the HIO and its participants, outlining the terms of the common interest to share data across the network members. An example of a flexible participation agreement is the Model Modular

Participants Agreement (MMPA). The California Office of Health Information Integrity facilitated the development of the Model Modular Participants Agreement (MMPA), designed to be easily tailored to meet both the governance and HIE technical architecture adopted by an HIO (MMPA Release 2.2.1, 2014).[3]

3.3. Business Associate Agreements

Contractually, health information exchange presents a complex landscape. What confuses the issue is the concept of a business associate agreement (BAA), raising two questions as to where and how it applies to the HIE landscape.

A business associate (BA) is defined under 45 CFR 161.103 as a person or entity that "creates, receives, maintains, or transmits protected health information" on behalf of a covered entity. A BA is not a member of the CE workforce. The definition extends to a "Health Information Organization[s], E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information" as well as "a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate" (45 CFR 160.103, 2013).

A **business associate agreement** (BAA) is a written contract between a covered entity and its business associate that contains the mandatory elements specified in 45 CFR 164.504(e). A BAA must also be established between a BA of a CE and any subcontractors that may be exposed to PHI. A BAA is unidirectional in nature, building a chain of trust that starts at the CE and extends first to the BAs of that CE and then the subcontractors of those BAs, depending on whether they handle PHI on behalf of that BA.

3.3.1. Question One: Where Does a BAA Apply?

Most participants in a HIE are either covered entities (i.e., a health plan, health care clearinghouse, or covered health care provider) or a business associate of a covered

[3] An example of an executed HIE/HIO participation agreement based on a version of the MMPA can be found at http://www.redwoodMedNET.org/projects/hie/docs/rmn_participation_20100225.pdf.

entity (such as ancillary service provider such as a laboratory) (45 CFR 160.103, 2013). While the US Department of Health & Human Services does not generally consider an HIO as a covered entity (CE), it does consider it a BA of its participants:

> "A HIO that performs certain functions or activities on behalf of, or provides certain services to, a covered entity which requires access to PHI would be a business associate under the Privacy Rule. See 45 C.F.R. § 160.103 (definition of "business associate"). [….] For instance, an HIO that manages the exchange of PHI through a network on behalf of multiple covered health care providers is a business associate of the covered providers, and thus, [according to 45 CFR §164.502(e)(1)(i)] one or more business associate agreements would need to be in place between the covered providers and the HIO" (U.S. Department of Health & Human Services, 2009).

Similarly, if the HIO discloses PHI to its subcontractors, such as the HIE technology vendor or hosting service, allowing the subcontractor to create, receive, maintain, or transmit PHI on the BA's behalf, the HIO must obtain satisfactory assurance that the subcontractor will appropriately safeguard that PHI per 45 CFR §164.502(e)(1)(ii). The BA must do so in compliance with 45 CFR §164.504(e)(1)(i) (45 CFR 164.502, 2013).

The result? At the network level, an HIO must enter into a business associate contract (BAA) with each participant that is a CE or a BA of a CE. An HIO must also enter into a BAA with each of its subcontractors. Generally, an HIO provides a BAA template as part of its participation agreement that can then be uniquely tailored by its Participants. Thus, an HIO may have multiple instances of its original BAA template associated with executed participation agreements.

However, there is an important distinction when discussing the relationship between HIOs that are participants in the highest level of a trust framework, a "network of networks" such as the national eHealth Exchange and the California Trusted Exchange Network (CTEN). A BAA is inapplicable because the relationship between the HIOs is bilateral. Rather than having a BAA between themselves, the HIOs act on behalf of their participants to facilitate inter-network exchange according to the DURSA.

The approach taken in the eHealth Exchange DURSA is to first restrict the exchange of information between two HIOs to a set of **Permitted Purposes.** These Permitted Purposes include further limits to HIPAA treatment, payment, and operations, public health activities and reporting, any purpose to demonstrate meaningful use of certified EHR technology and uses and disclosures based on an individual's authorization. This, in effect, provides an escape clause for having to execute BAAs between HIOs in conjunction with the DURSA. Specifically, the DURSA is not intended to serve as a BAA among its Participants as the Participants are limited to exchanging information only for a Permitted Purpose, implying that "Participants do not intend to become each other's Business Associate" (Citation needed here). The DURSA does establish HIPAA as a contractual standard of performance for Participants that are not otherwise subject to HIPAA (e.g., CE, BA of a CE, or Governmental Participant.) (The Sequoia Project, n.d.).

3.3.2. Question Two: What Should Be in a BAA?

45 CFR §164.502(e)(2) provides that the satisfactory assurance described above must be in a written contract or other written agreement or arrangement with the business associate that complies with the mandatory and optional BAA provisions laid out in 45 CFR §164.504(e) (45 CFR 164.502, 2013).

However, many healthcare- covered entities leverage the BAA as a form of contractual service level agreement that addresses topics that are outside the regulatory purposes of a BAA. An HIO needs to watch for and evaluate provisions that tend to creep into a BAA but are not required by HIPAA regulation (Salyers). "BAA abuse" can make this contractual agreement a regulatory and contractual "kitchen sink." BAA abuse is dangerous in a complex data sharing environment such as HIE where an HIO may have to sign different BAA with multiple participants (Hinkley & Briskin, 2016). BAA abuse makes it hard for the HIO to comprehend and manage all its HIPAA contractual obligations.

The closer a BAA is modeled to the mandatory requirements of the HIPAA rule, the easier it will be to administer. For BAAs that diverge from the provisions laid out in HIPAA, legal counsel cannot easily rely on HIPAA to clarify any interpretations for concepts such as “consent,” “authorization,” “breach,” or when “security incident” is “discovered” or “should have been discovered”. This can raise operational concern over whether the policies and procedures (P&Ps) of the BA satisfy BAA requirements.

BAAs that are part of a HIE trust framework should not be stand-alone, but attached to a parent agreement (i.e., an inter-HIO agreement such as a DURSA, participation agreement, or contract) and should align with, not duplicate, the terms in the parent agreement.

The nuances of the relationship between the HIO, its participants, and its subcontractors can and should be clearly delineated in the vendor contract, the participant agreement, or the service agreement according to the role and relationships involved.

The order of precedence across related documents should be clearly understood and established. For example, a BAA may take legal precedence over the parent material. One can strive to avoid this issue by first examining the clauses in each related document for consistency and then updating to avoid conflicts. A clause can then be written to state that, as of a given date, the documents are considered consistent with each other, and there is effectively no order of precedence among them.

Operational details can then be established in support of these documents through supporting policies and procedures. Details, such as determining order of precedence of documents or clarification of Permitted Purposes, can be developed to meet the requirements raised by each of these relationships and harmonized across the HIE and its participants as a whole.

3.4. Policy and Procedures

In a HIE trust framework, the higher level agreements (i.e., the DURSA and the participation agreement) incorporate the HIO policies and procedures (P&Ps) by reference. The P&Ps must bring together flow-down provisions, conflicts and exceptions due to regulation and law, and guidance released by Office of Civil Rights (OCR) in the interpretation of HIPAA, such as the recently release OCR guidance on cloud computing under HIPAA (Office of Civil Rights, 2016).

Developing a set of harmonized HIO policies and procedures, however, is difficult for several reasons. First, how should the policies and procedures adequately reflect the concept of "applicable law"? The eHealth Exchange flow-down provisions contained in Table 1 exemplifies some of the challenges, such as complying with applicable law and breach notification. Within the United States, the HIPAA Privacy and Security Rules provide a common floor for standard policies and practices governing the sharing of ePHI, but even at the Federal level, there are significant conflicts between HIPAA and other federal privacy statutes, such as 42 CFR that regulates confidentiality around substance abuse. State law also often requires more stringent controls around highly sensitive information, such as HIV/AIDS and mental health and more onerous breach reporting requirements (Filkins, 2012).

Data breach law is also not consistent across jurisdictions. As a state, California is famous both for being the first state in 2003 to require security breach notification (SB 1386) as well as continually amending its statutes. For the third time in as many years, the Golden State continued this tradition of leadership and change in 2015 by taking three separate legislative actions, each one amending a different aspect of California's breach notification framework (Koller, 2015).

Table 1: DURSA Flowdown Provisions (The Sequoia Project, n.d.)

Section 15.01: Establish valid and enforceable agreements or user policies with participating organizations or users that:	Section 15.05. Establish valid and enforceable agreements or user policies with participating organizations or users that:
• Comply with all Applicable Law • Reasonably cooperate with the Participant on issues related to the DURSA • Comply with Permitted Purpose • Use data in accordance with DURSA • 1 hour for likely breach alert/24 hour for breach determination • Protect passwords or other security measures issued by the Participant	• Comply with all Applicable Law • Protect privacy and security of data/message content • Breach notification as soon as reasonably practical • Reasonably cooperate with other Participants on issues related to the DURSA

An HIO would be well- advised to engage legal counsel to evaluate the restrictions on privacy and security required by all elements of “applicable law.” This should include both a review of applicable Federal statutes as well as any conflict with state legislation. Given the clinical nature of the information being used and exchanged by HIE participants, HIO policies and procedures may need to address other regulations like Clinical Laboratory Improvement Amendments (CLIA) (Clinical Laboratory Improvement Amendments (CLIA), 2016) and Comprehensive Addiction and Recovery Act (CARA) (Laff, 2016).

Second, the HIO needs to harmonize its P&Ps with those of its participants, each having policies that affect how they will interact with the HIE. Definitions can vary – the meaning of ‘administrator’ for the HIE is not necessarily the same as for the hospital EHR that is providing or consuming data. Access rights will vary and may not map smoothly across primary care providers and their behavioral health counterparts due to privacy concerns. Particularly for Centralized HIEs, the trust framework must attempt to harmonize often disjointed rules by establishing the proper level of policy (Filkins, 2012).

Third, another major factor in P&P implementation is patient consent. There are a variety of consent models, usually opt-in or opt-out, with various levels of granularity. A provider may have a patient sign an authorization consenting to the disclosure of his orher records in accordance with the applicable HIE data exchange policy, based on applicable law (Filkins, 2012).

Two basic HIE architectural models influence the development of a trust framework through the impact on policies and procedures. **Directed Exchange** represents “point-to-point communication between known endpoints, whether represented as established routes for Health Level 7 (HL7) message delivery (using various transport methods) or secure email (based on S/MIME) between providers with verified identities” (Filkins, 2012). **Query-based Exchange** implies an architecture where a user queries the HIE for patient data that has been gathered and normalized across various external data sources. Results are delivered either from a centrally located clinical data repository (CDR) (**Centralized HIE**) or via a virtualized record using a record locator service (RLS) (**Federated HIE**). **Error! Reference source not found.** presents an overview of these two basic types and common variations:

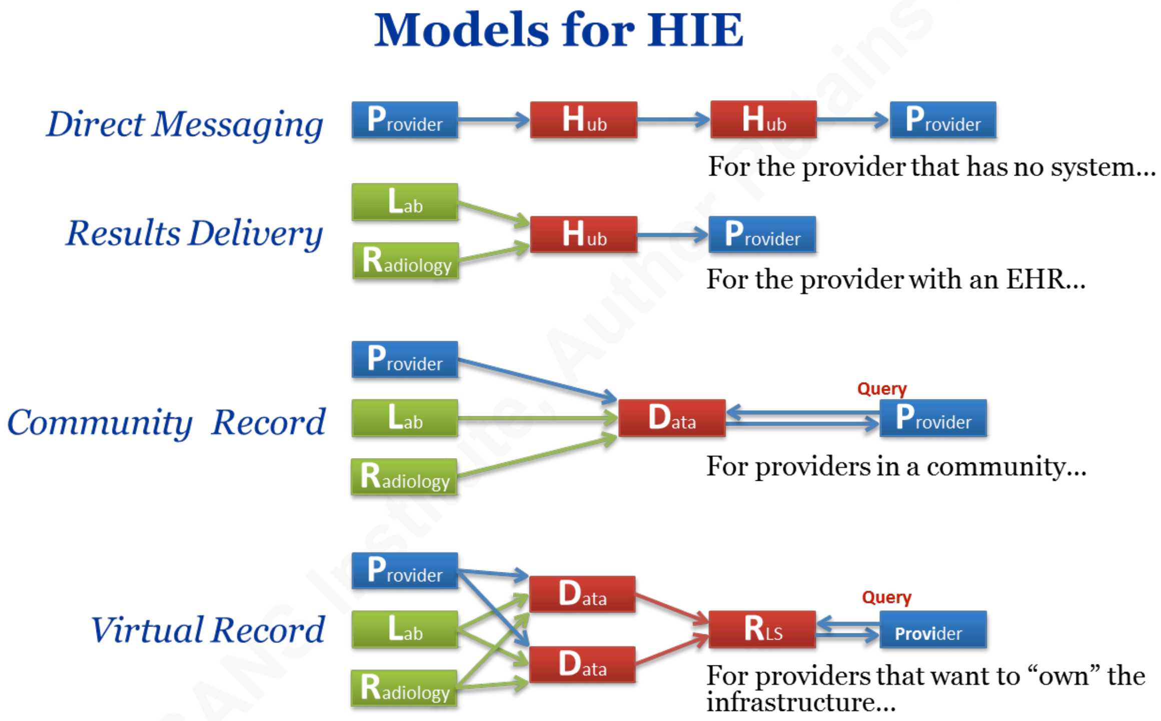

Figure 4: HIE Architectures and Variations (Cothren, 2014)

Policy development and enforcement is easier in Directed Exchange. It is more challenging in Query-Based Exchange. In the former, the HIE does not have to manage patient consent as it is assumed to be implicit in the transaction. The healthcare provider asks the patient for his orher consent before initiating any transfer so that the resulting transaction occurs directly from one provider to another known provider in accord with patient expectations (Filkins, 2012).

In Query-Based Exchange, however, the patient's data sharing preferences (i.e., patient consent) are stored in a location so that when queried data is provided, only those data elements consistent with patient privacy preferences are shared for that request. The corresponding Notice of Privacy Practices must state the legally permitted purposes for which the data can be used. Secondary disclosure is difficult in the case of conflicting or overlapping consents if the patient has been seen by several providers throughout a community and for different reasons (Filkins, 2012).

Finally, HIE is not represented by a discrete endpoint to the user, such as an electronic health record system, database or portal. Rather, a HIE functions more like a set of network-based services to transform data, match patient and provider identities, apply permissions (access, rules of behavior related to consent), route, monitor and manage. Direct access to CDR records is also likely to be invisible to the end-user, integrated into their native EHR system access. What is 'tangible' to the end user, however, is the data that the HIE exchanges, how it is classified, and how it is used.

The HIPAA Security Rule requires that a risk assessment be completed. This activity should inform the policy decision-making process. HIE policy development should also be based on risk, but the risk assessment has different characteristics. It is not based on an inventory of critical assets that includes physical hardware, software, and paper-based data. Rather it must take into account the transaction patterns and permitted uses for the data, the complexities of data governance, and the HIE architecture (Directed or Query-based) that identifies threat-vulnerability pairs. It will need to emphasize operational processes such as change management, risk assessment and management, incident response, and cyber defense as controls to mitigate concerns over privacy and security.

4. The Implementation Scenario

The demand for data integration and sharing among unaffiliated healthcare entities is growing within certain a California county ("the County"). The geography, population size, and widespread adoption of Electronic Health Records (EHRs) and related information technology infrastructure throughout the County's region position it well for the use of HIE.

An HIO has been established to implement a governance structure that represents the interests of the various County stakeholders in the Community Health eXchange (or simply eXchange). A primary objective of this governance structure is to create the applicable trust framework for this County HIE. The trust framework includes the following elements: 1) tailoring the legal and contractual agreements to meet the business and operational needs, 2) evaluating technical demands and service needs, and 3) developing policies and procedures that collectively allow the community HIE to strive to meet regulatory and jurisdictional privacy and security requirements – federal, state, and local -- as well as those boundary conditions of eXchange Participants, especially those entities that must coordinate patient care across medical and mental health clinics.

Figure 5 shows the current organizational, legal, and contractual, relationships, among the eXchange stakeholders. The eXchange HIO is being incubated under the County Health and Human Services (HHS) Agency with an eventual goal of transitioning to a private, independent entity, much as the ONC transitioned the NwHIN to the Sequoia Project. The eXchange HIO does not provide any technical services, although they (or their participants) remain responsible for policy-related operations that are directly related to the technical, including access management, data quality and integrity, and auditing. The HIO has contracted with another HIO, the Clinical Care Network or ClinCareNET, to serve as both the system integrator for the eXchange and the hosting service provider for an initial duration of three years. The eXchange, still in the design and development stage, follows a Centralized HIE model.

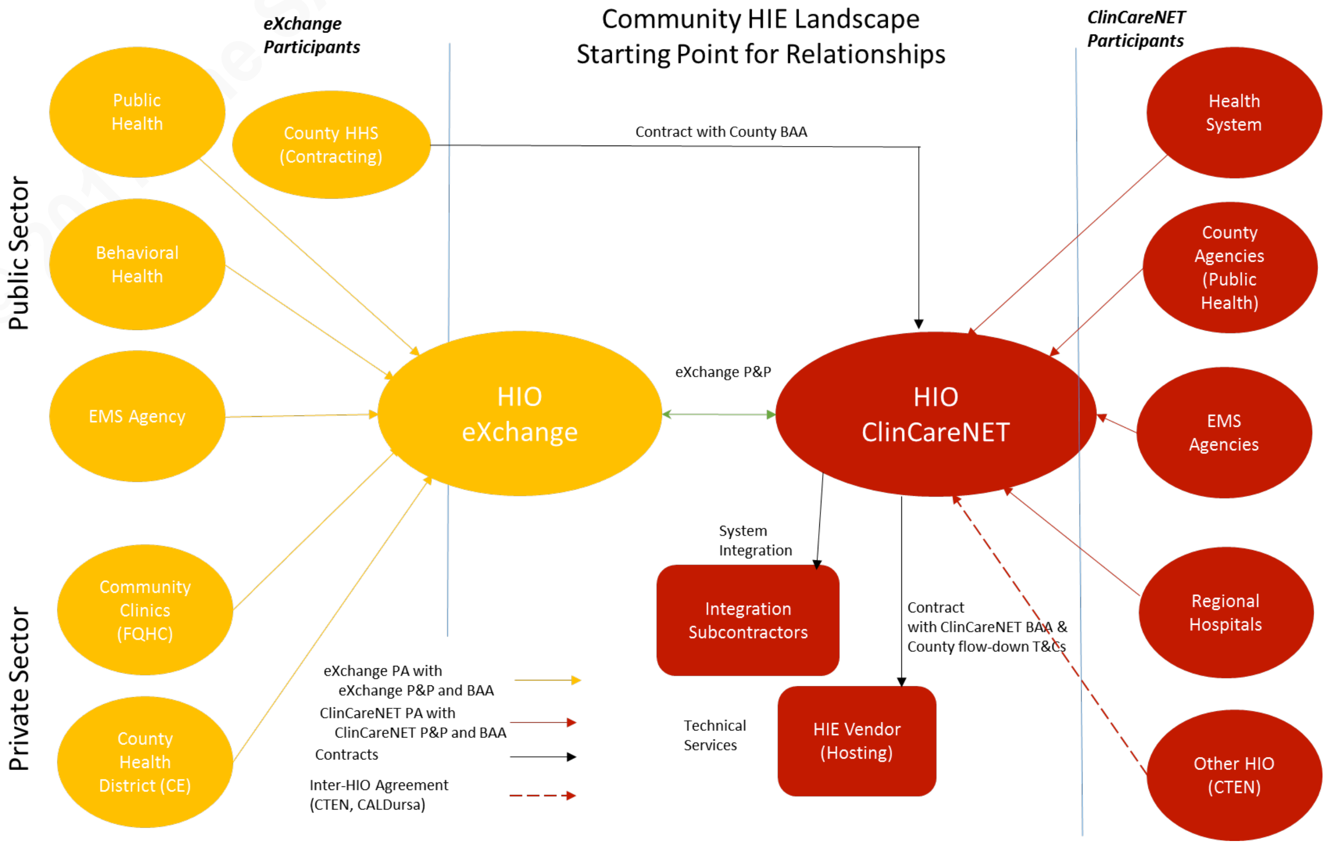

Figure 5: The Starting Point for the eXchange Trust Framework

5. Implementation Challenges

As governance is underway, eXchange participants are realizing some of the problems in implementing a trust framework for this HIO. This section describes three major challenges and offers recommendations for how to mitigate each.

5.1. Challenge #1: Resolving Governance Gaps

Recall one of the reasons for a DURSA (or inter-HIO) agreement is the ability to share data bilaterally across two networks. As an HIO, ClinCareNET provides oversight, governance, and value-added services to its own participants, under its own Participation Agreement, with its own BAAs and policies and procedures. It is also a member of the California Trusted Exchange Network and can share its patient data with the other signatories of the CTEN DURSA (i.e., CalDURSA). However, it is only considered a vendor in relation to the eXchange HIO with a contract and accompanying BAA. Also, of note that while ClinCareNET is a member CTEN member, the eXchange has not on-boarded to the CTEN.

Several organizations that are ClinCareNET participants overlap with those of the eXchange regarding geographic coverage and patients served but are not eXchange participants. A patient with longitudinal records in both the eXchange CDR and the ClinCareNET CDR receives care at the GIAC Health System Community Hospital in the County. The Community Hospital and the GIAC Health System to which it belongs participate in ClinCareNET but not in the eXchange. The staff at the Community Hospital are aware that there is more information about the patient in the eXchange and want to access that information in addition to what they can access in ClinCareNET.

As its own HIO, ClinCareNET can push the data it holds on behalf of ClinCareNET participants to ClinCareNET participants. As a vendor to the eXchange, it can push the data it holds on behalf of eXchange participants to eXchange participants. It cannot, however, push ClinCareNET data to eXchange participants or vice versa, even if the patient involved is the same person.

One of two actions must happen before the data are exchanged:

1) The eXchange joins (i.e., onboards to) a network, such as CTEN or the ehealth Exchange, that has a legally vetted DURSA. It will then be able to exchange the patient information with other network members, that includes the Community Hospital if the Hospital or its parent Health System. Which network the eXchange joins will be a business decision based on business-related needs, resources, and costs. The cost to onboard to eHealth Exchange is, for example, significantly higher than onboarding to the CTEN, but may be cost beneficial in the long term as joining the national network will allow the eXchange to interoperate with national health enterprises like Kaiser or Federal agencies like the United States Veterans Administration.
2) ClinCareNET and the eXchange execute a local interHIO agreement that opens each up to sharing each other's patient data or, possibly, allows ClinCareNET to provide "pass-through" access to CTEN for this (or similar) patients. The disadvantage is that this would be an independent agreement and may not have been as completely legally vetted and operationally accepted by a larger community as has the DURSA or CalDURSA has. The eXchange would remain in charge of scope, time, and cost in developing this agreement, but the relationship would remain "local" and would not allow access to other larger networks.

The data boundary between the two HIOs needs to be crystal clear and not confused with the vendor relationship between ClinCareNET and the eXchange. Data belonging to each HIO is appropriately segmented and secured in the ClinCareNET CDR from both policy and technical standpoints. The trust framework is lacking an inter-HIO agreement dealing with that exchange between the two HIEs. This lack of an agreement should be viewed as a gap in data-sharing trust, which should be reviewed by HIO Governance and then resolved through a business decision.

5.2. Challenge #2: The BAA Conundrum

The existing trust framework for the eXchange contains a maze of BAAs associated with the executed agreements and contracts.

5.2.1. Where Does a BAA Apply?

A question of whether all needed BAAs between the eXchange and its Participants are in place needs to be resolved before the flow of live PHI can occur electronically.

The first issue is whether all the actors are properly classified as CEs, BAs, or ‘other.' ClinCareNET has a long-standing relationship as a business associate with its participants, which are all covered entities. On the eXchange side, all participants, both public and private, have signed the Participation Agreement, modeled on the MMPA, along with the BAA that establishes an agreement between that participant (where that participant is a CE) and the eXchange, as a business associate of that CE.

However, the County has neglected to fully define the relationship between HHS and the eXchange. Technically, the eXchange, as an HIO will not be a CE but will be a BA of HHS, the County CE. As both the eXchange and HHS are government entities, such a relationship needs to be established by a memorandum of understanding (MOU) between two government entities – HHS and the eXchange – until such time that the eXchange becomes a free-standing legal entity and the MOU is replaced by a BAA (45 CFR 164.502, 2013).

Next, ClinCareNET has executed a County contract, including a related County BAA, with the County HHS Agency, which has agreed to act as the contracting organization for the eXchange. This establishes an agreement between the County HHS and ClinCareNET, as a general business associate providing system integration services and operations for the eXchange. However, there is a perceived risk as to the relationship between ClinCareNET and the private entities that are participating in the eXchange.

These private entities are clinics that are entirely independent of the County, except for their participation in the eXchange. Consequently, a separate, interim, standalone BAA should be executed between ClinCareNET and the clinics, until superseded by an inter-HIO agreement between the ClinCareNET and eXchange HIOSs that also references a BAA.

5.2.2. What Should a BAA Cover?

The BAAs used by the eXchange are consistent in that each is based on a template from a single source, a collaboration of stakeholder and County counsels. However, the terms of the form represent the "BAA abuse" cited earlier in Section 3.3.2. Here are four examples of terms in the form that constitute "BAA abuse:"

- **Indemnification and Insurance.** The BAA includes terms around indemnification and hold harmless. HIPAA does not require that a BAA support indemnification. These conditions should be removed and addressed in the related parent agreement (e.g., PA, vendor contract). For example, if these terms are deleted from the BAA and put into the parent agreement, then any breach of security by the business associate would be treated as a breach by a vendor, and the vendor will be held responsible under terms applicable to a vendor.
- **Reasonable Cooperation:** The HIO needs to be careful that a requirement for reasonable cooperation does not translate to over-involvement by any particular participant, especially a CE, in the HIO's operational or compliance programs. The HIO must harmonize its operations, compliance, and policies across a variety of participants.
- **Unreasonable Deadlines:** Unworkable deadlines can limit the effective working relationship needed between the HIO and it participants as well as it vendor ClinCareNET. A good rule of thumb is to allow 15 business days for most deadlines. Examples of where unreasonable deadlines can become a disaster include: reporting unauthorized uses and disclosures, reporting data breaches, determining if "suspected" events have occurred, providing an accounting of disclosures, providing access, making amendments, and curing defaults.
- **Over-reporting Incidents:** While HIPAA requires a BA to report both successful and unsuccessful incidents, it does not set time limits for such reporting, although governing or applicable law may have requirements. HIPAA also does not require the same approach nor the same period for reporting successful versus unsuccessful. The HIO should agree to report successful incidents promptly and

in detail, while unsuccessful incidents can be aggregated and reported on in a periodic fashion.

Finally, not only should the basic BAA template used by the HIO align with HIPAA provisions, but also there should not be any freestanding BAAs involving the HIE. The parent agreement (DURSA, PA, SLA, or contract) should reflect the legal nuances engendered by that role.

5.3. Challenge #3: Operationalizing Policies and Procedures

The eXchange must establish operational procedures to ensure compliance with its P&Ps, provide appropriate training, and require acknowledgment from its participants and their end users as to common terms and conditions before ePHI is exchanged or disclosed over the HIE. The HIO understands the need to focus on data in evaluating threats and vulnerabilities, limitations and constraints that will dictate the approach to subsequent data governance to ensure that the terms and conditions of the trust framework and its agreements can be met, managed, and maintained.

Scenarios for exchange are also needed to understand where, when, and how the data held by the HIE will be accessed, exchanged, and stored. A narrative description that tells a story familiar to its participants is often the best starting point. These scenarios then need to be decomposed into operational workflows using methods such as cross-functional or "swim lane" diagrams. Diagrams should explain, at a minimum, 1) participant roles that will access the data in the HIE, 2) the edge systems (source and destination) that will provide and/or receive the data, 3) confirmation these activities represent "permitted purpose" or "uses" in alignment with the trust framework agreements, and 4) identify any policies and procedures that need to be added or updated.

Concurrent with this exercise is classifying the data at the individual data elements, attribute, and metadata levels, as well as any information, derived, in accordance with its sensitivity, value, and criticality. A resulting classification scheme should be established in policy to determine and evaluate what safeguards around the data and information will be necessary. These safeguards should not only address encryption at rest and in transit, but also de-identification techniques to preserve privacy and reduce the risk of patient re-identification.

Data boundaries should be viewed as system boundaries in the world of HIE. As a Centralized HIE, the eXchange stores data remotely in a cloud-based CDR, making it difficult to establish a hard network-based security perimeter. Workflow or process-based scenarios can be developed and reviewed against one another with the proposed implementation architecture. These scenarios can identify areas of potential concern and determine where to place effective, policy-based controls, both administrative (written) and technical (network-based) to mitigate operational risk.

The UML sequence diagram in Figure 6 is an example of this scenario-based analysis. The diagram shows the flow of patient demographic (ADT) information from the EHR through the locally hosted eXchange infrastructure to its cloud-based HIE service stack that includes the Master Patient Index (MPI) and the CDR. Intermediate actions are taken on the data (filter, transform, and match to a patient identity) by each system or service as the data is progressing to its final storage in the cloud.

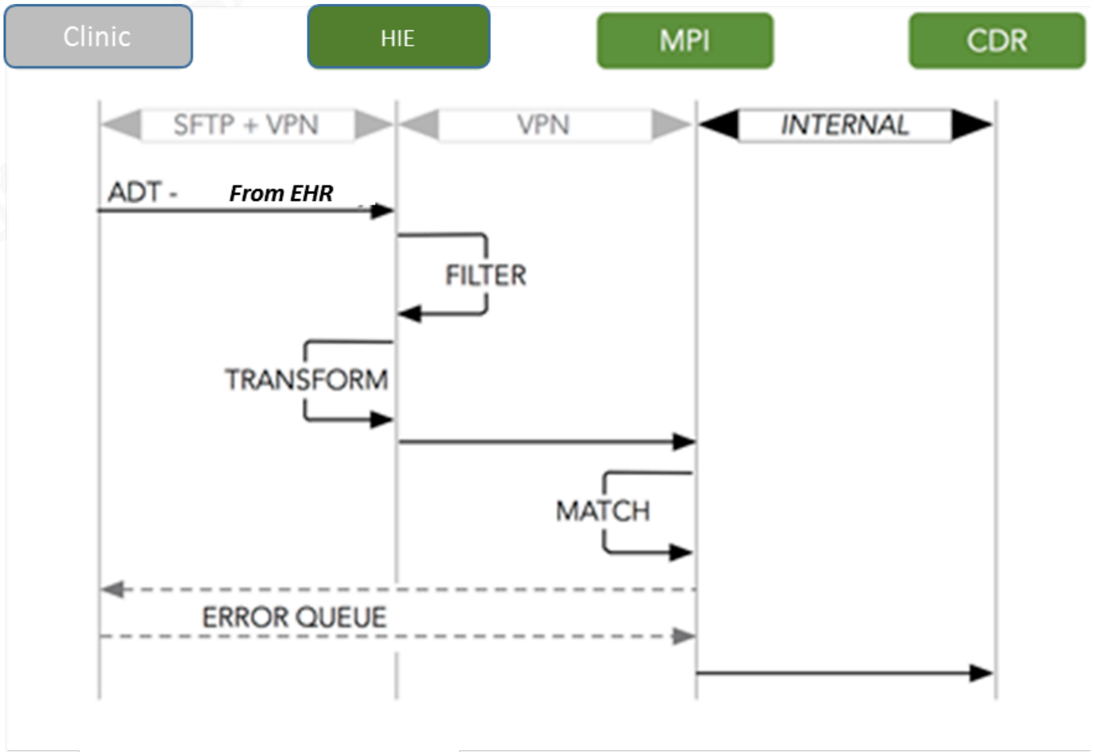

Figure 6: Sample UML Sequence Diagram for Policy Analysis

The eXchange HIO has determined that, as part of its data governance policy, all data must be encrypted both in transit and at rest, including any intermediate storage. The diagram shows the processes that will encrypt the data in transit (SFTP and VPN), but it does not appear that the ADT data will be encrypted by ClinCareNET (the HIE) while in intermediate storage during the filtering and transformation processes according to the HIO policy. Such encryption should be implemented by the HIE as a process along with the filtering and transformatiom, and shown on this diagram, in support of the data classification and protection policy.

6. Recommendations for the Future

As the world moves further into the digital universe – the sharing of health data across unaffiliated entities will not slow down. The rise of value-based incentives and population health demands that providers place trust in the validity, accuracy, and completeness of data. Heath care tailored to the individual such as with precision medicine raises new and chilling privacy scenarios at the genomic level. Technology is becoming faster, smaller, and more pervasive with the rise of the Internet of Things.

While the approaches to solve the implementation challenges discussed in this paper may appear simple they can be difficult to actually achieve. The following recommendations are also potentially wide- reaching with application beyond the particular use case described in this paper.

Recommendation One: HIO governance is the starting point to establish the trust required for exchange, setting the foundation for defining, understanding and implementing HIE privacy and security issues. A comprehensive review of possible use cases, even the ones that might appear insignificant at first appearance, need to be examined and the appropriate agreements established to cover all possible relationships between the principal actors.

The use case in this paper highlights the need to execute an inter-HIO agreement between the two HIOs to avoid any governance gaps related to inconsistent access to patient information across the community.

Recommendation Two: Evaluate all contractual relations but specifically those related to business associate agreements. Potential conflicts in the eXchange use case can be resolved by evaluating the approach to business associate agreements, including:

1. The need for a BAA at the inter-HIO (i.e., network-to-network level) given that not all HIOs are HIPAA-related entities,
2. Standardizing all BAA terms that support the trust framework of a particular HIO, and
3. Keeping the BAA as close to the mandatory and optional terms in the HIPAA Rule as possible.

Finally, strive for consistency across the related documents and agreements to avoid any issues that might be associated with the order of precedence.

Recommendation Three: Expand privacy and security risk management to account for a needed emphasis on the data and information being exchanged by the HIE, not just on the information technology, pipes, and platforms that may no longer be directly under the control of Participant IT shops. Traditional privacy and security risks must be balanced with the risk to data quality, usability, and integrity standards the HIO must uphold for the delivery of patient care.

A formal approach to data governance is needed that focuses holistically on a variety of concerns related to privacy, security, and compliance from the perspective of information and data, not from the standpoint of IT and architecture. Understanding legal and contractual elements in health information exchange informs how trust can be developed and improved for other related areas in health such as clinical trial networks, where researchers, medical providers, and patients work towards new treatment options for improved clinical outcomes.

7. References

45 CFR 160.103. (2013, January 25). Retrieved February 17, 2017, from Legal Information Institute: https://www.law.cornell.edu/cfr/text/45/160.103

45 CFR 164.502 . (2013, January 25). Retrieved February 10, 2017, from Legal Information Institute: https://www.law.cornell.edu/cfr/text/45/164.502

AHIMA/HIMSS HIE Privacy & Security Joint Work Group. (2011, April). *The Privacy and Security Gaps in Health Information Exchanges.* Retrieved from AHIMA: http://library.ahima.org/PdfView?oid=104470

CalINDEX. (2016). *CalINDEX*. Retrieved February 9, 2017, from CalINDEX: https://www.calindex.org/

Clinical Laboratory Improvement Amendments (CLIA). (2016, December 5). Retrieved February 10, 2017, from Centers for Medicare and Medicaid: https://www.cms.gov/Regulations-and-Guidance/Legislation/CLIA/index.html

Cothren, R. (2014, April 24). *An Update on HIE in California.* Retrieved from Califonria Institute for Behavorial Health Solutions: http://www.cibhs.org/sites/main/files/file-attachments/thurs_11_15_chicago_a_current_update_r.cothren.pdf

Data Use and Reciprocal Support Agreement (DURSA). (2017). Retrieved from http://sequoiaproject.org: http://sequoiaproject.org/wp-content/uploads/2017/01/Restatement_I_of_the_DURSA_9.30.14_final.pdf?x54807

Dierker, L. (2008). State Connection: State-level Efforts in Health Information Exchange. *Journel of AHIMA*, 40-43. Retrieved from http://library.ahima.org/doc?oid=80242#.WJ1N0o0m6Uk

Filkins, B. (2012, October 7). *Incident Handling in the Healthcare Cloud: Liquid Data and the Need for Adaptive Patient Consent Management.* Retrieved from SANS: https://www.sans.org/reading-room/whitepapers/hipaa/incident-handling-healthcare-cloud-liquid-data-adaptive-patient-consent-ma-34007

HealthIT.gov. (2014, May 12). *What is HIE?* Retrieved from HealthIT.gov : https://www.healthit.gov/providers-professionals/health-information-exchange/what-hie

HIMSS. (2013, April 5). *Definition of Interoperability.* Retrieved from HIMSS: http://www.himss.org/sites/himssorg/files/FileDownloads/HIMSS%20Interoperability%20Definition%20FINAL.pdf

HIMSS FY16 HIE inPractice Task Force. (2016, June 4). *HIE Patient Engagement Case Study: Kaiser Permanente*. Retrieved from HIMSS: http://www.himss.org/hie-patient-engagement-case-study-kaiser-permanente

Hinkley, G., & Briskin, A. (2016). Business Associate Obligations and Agreements: Aftermath of the HIPAA Omnibus Rule. Pillsbury Withrop Shaw Pittman LLP.

Information Sharing Environment. (n.d.). *Establishing Trust and Interoperability in the Information Sharing Environment*. Retrieved from Information Sharing Environment : https://www.ise.gov/mission-stories/standards-and-interoperability/establishing-trust-and-interoperability-information

Klepper, B. (2013, October 18). *Facilitating Interoperability*. Retrieved from Health Affairs: http://healthaffairs.org/blog/2013/10/18/facilitating-interoperability/

Koller, M. S. (2015, October 12). *California Amends Its Breach Notification Statute*. Retrieved from Data Privacy Monitor: https://www.dataprivacymonitor.com/data-breach-notification-laws/california-amends-its-breach-notification-statute/

Laff, M. (2016, November 9). *Variety of State Regulations Take Aim at Opioid Abuse* . Retrieved from American Academy of Family Physicians: http://www.aafp.org/news/government-medicine/20161109stateconfopioids.html

McCarthy, J. (2017, January 6). *A guide to interoperability at HIMSS17*. Retrieved from HIMSS: http://www.healthcareitnews.com/news/guide-interoperability-himss17

Middleton, B. (2008, October 1). *Value propositions for community health information exchange include many voices but one vision* . Retrieved from Managed Healthcare Excutive: http://managedhealthcareexecutive.modernmedicine.com/managed-healthcare-executive/content/value-propositions-community-health-information-exchange-includ

MMPA Release 2.2.1. (2014, April 1). Retrieved from CAHIE: http://www.ca-hie.org/2014/04/mmpa-release-2-2-1/

National HIE Governance Forum. (2013, December). *Trust Framework for Health Information Exchange.* Retrieved from HealthIT: https://www.healthit.gov/sites/default/files/trustframeworkfinal.pdf

Nationwide Health Information Exchange (HIE) Resources. (2013, January 22). Retrieved from HealthIT: https://www.healthit.gov/policy-researchers-implementers/nationwide-health-information-exchange-hie-resources

Office of Civil Rights. (2016, October 6). *Guidance on HIPAA & Cloud Computing*. Retrieved February 10, 2017, from US Department of Health & Human Services: https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html

Salyers, J. C. (n.d.). *BAC to the Basics: Business Associate Contracts Made Easy.* Retrieved from Context Law: http://www.bssdlaw.com/files/business_associate_contracts.pdf

San Diego Health Connect. (n.d.). *Who We Are*. Retrieved February 9, 2017, from San Diego Health Connect: http://sdhealthconnect.org/About_SDRHIE/who-we-are.html

The National Alliance for Health Information Technology. (2008, April 28). *Report to the Office of the National Coordinator for Health Information Technology.* Retrieved from HITECH Answers: http://www.hitechanswers.net/wp-content/uploads/2013/05/NAHIT-Definitions2008.pdf

The Sequoia Project. (n.d.). *About the Sequoia Project*. Retrieved from The Sequoia Project: http://sequoiaproject.org/about-us/

The Sequoia Project. (n.d.). *Data Use and Reciprocal Support Agreement (DURSA)*. Retrieved from The Sequoia Project: http://sequoiaproject.org/ehealth-exchange/onboarding/dursa/

U.S. Department of Health & Human Services. (2009, December 15). *Is a health information organization (HIO) covered by the HIPAA Privacy Rule?* Retrieved from Health Information Privacy: https://www.hhs.gov/hipaa/for-professionals/faq/559/is-an-hio-covered-by-hipaa/index.html

Appendix A
Acronyms

Acronym	Description
ADT	Admission, Discharge, Transfer
AHIMA	American Health Information Management Association
AIDS	Acquired Immune Deficiency Syndrome
BAA	Business Associate Agreement
CDR	Clinical Data Repository
CE	Covered Entity
CFR	Code of Federal Regulations
CMIA	California Confidentiality of Information Act
CTEN	California Trusted Exchange Network
DURSA	Data Use and Reciprocal Sharing Agreement
EHR	Electronic Health Record
EMS	Emergency Medical Services
ePHI	Electronic PHI
HHS	Health and Human Services
HIE	Health Information Exchange
HIMSS	Healthcare Information and Management Systems Society
HIO	Health Information Organization
HIPAA	Health Insurance Portability and Accountability Act,
HITECH	Health Information Technology for Economic and Clinical Health Act
HIV	Human Immunodeficiency Virus
HL7	Health Level 7
MMPA	Modular Model Participation Agreement
MOU	Memorandum of Understanding
MPI	Master Patient Index
NwHIN	Nationwide Health Information Network
OCR	Office of Civil Rights
ONC	Office of National Coordinator
P&Ps	Policies and Procedures
PA	Participant Agreement
PHI	Protected Health Information
RLS	Record Locator Service
SB	Senate Bill
SLA	Service Level Agreement
UML	Unified Modeling Language
US	United States