Global Information Assurance Certification Paper

Incident Handling in the Healthcare Cloud: Liquid Data and the Need for Adaptive Patient Consent Management

GIAC (GCIH) Gold Certification

Author: Barbara Filkins, filkins@impulse.net
Advisor: Hamed Khiabani

Accepted: October 7, 2012

Abstract

Privacy has been, and will remain, a leading business driver for security in healthcare. The sharing of sensitive patient records is protected by regulatory, jurisdictional, and organizational polices as well as individual patient consent, all of which form a foundation for behaviors associated with medical data. Patient preferences articulate a set of exceptions that, together with these other factors, become the rules by which medical information is shared and disclosures tracked as well as the definition for what is considered a breach.

This paper explores the concept of adaptive patient consent as a protection and tool for incident handling from several angles: the business need, the specification of functional and technical requirements, and the development of a reference architecture that involves the various components of standard security architecture, repurposed as an adaptive patient identification and consent management solution for heath care information privacy and security in the cloud.

1. Introduction

The increasing use of electronic health record (EHR) systems, health information exchange (HIE) networks, and cloud computing significantly increases the exposure of sensitive medical information to loss of confidentiality, integrity, and availability due to data-related attacks, such as medical identity theft or insider threats (Ponemon Institute, 2011). Yet, the healthcare community is willing to accept these risks for the greater advantages of reduced cost, rapid provisioning, and elasticity of service with access to information and knowledge readily available at the point of patient care.

Liquid data needs adaptive protections; the rules for data access, such as determined by patient consent, need to flow with the data being protected. The challenge of how to incorporate data-centric permissions and controls in cloud-based architectures for healthcare is not simple, adding to the complexity of an industry that is already overwhelmed by its struggles with syntax and semantics in coded data.

This paper explores how patient consent management can help achieve increased privacy and security for clinical data in a cloudy world, using high-level requirements analysis and reference architecture development. The analysis uses requirement levels normally defined in the software engineering domain (Wiegers, 2003). Sections 2 and 3 cover the business and user requirements respectively. Section 4 discusses functional or behavioral requirements and non-functional or technical requirements. Section 5 lays out a reference architecture which sets these functional and technical requirements into perspective. Section 6 summarizes findings and thoughts for the future.

2. The Business Need: Healthcare in the Cloud

The American Health Information Management Association (AHIMA) defines *health information exchange* as:

"Health Information Exchange refers to the process of reliable and interoperable electronic health-related information sharing conducted in a manner that protects the confidentiality, privacy, and security of the information" (AHIMA, 2012).

Within the healthcare industry, the term HIE tends to be used both as a verb to describe the process of exchange and as a noun to refer to the technical standards and infrastructure that support that exchange. However, it is the HIE infrastructure, not necessarily the process, that serves as a lens through which many participating healthcare organizations assess the sharing of electronic protected health information (ePHI), whether in their role as data owner or data custodian. Organizations pondering HIE participation express concern with the release of what they consider "their" data to an HIE network as the data is no longer under their direct control. On the other hand, most HIE participants still share ePHI as if the full infrastructure were under their control, not fully acknowledging extent to which cloud-based computing decouples the infrastructure from the actual data and the potential for increased risk associated with breaches of confidentiality or loss of integrity.

Incident response is the "organized approach to addressing and managing the aftermath of a security breach or attack (also known as an incident). The goal is to handle the situation in a way that limits damage and reduces recovery time and costs" (Rouse, 2012). For a cloud-based HIE network, incident response must transcend the boundaries of any one organization and deal with attacks on data, largely independent of the underlying technical infrastructure and participant systems and networks.

Thus, the solution presented in this paper starts with two key business requirements associated with the need to secure sensitive clinical information in a cloud-based HIE: 1) develop an approach for how data released to an HIE network might be protected in accordance with established policy and patient consent and 2) how the HIE infrastructure can provide controls around sensitive data to ensure that data is being protected in accordance with those policies.

3. The User Perspective: Concepts in Action

User requirements represent "what users will be able to do with the system" (Wiegers, 2003, p. 6). Success or failure of an information system solution is often directly proportional to how well the customer expectations were realized by the solution. This section will present several basic concepts related to the process of HIE, provide a

simple scenario that that outlines how end users would interact with an HIE network, and conclude with a discussion around incident response and consent management.

3.1. Basic Concepts in Health Information Exchange

On March 22, 2012, the ONC released a program information notice (PIN) delineating requirements for establishing a privacy and security framework for HIE (ONC, 2012). In this document, the ONC defined the two main architectural approaches towards HIE being taken today:

- **Directed Exchange** where the HIE infrastructure serves solely as information conduits for the transfer of ePHI between two designated and verified endpoints and does not access or use the data beyond what is required to encrypt and route it.
- **Data Aggregation** in which the HIE infrastructure stores, assembles or aggregates individually identifiable health information, whether centrally or in a federated model. Typically, this type of HIE network holds patient information in a clinical document (or data) repository (CDR) accessible by HIE- authorized sources and users.[1]

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. Information is considered as being "pushed" from a source to a receiver, whether the source and receiver are systems or individuals. Directed Exchange implies that patient consent has been initiated by the fact that the ePHI is being pushed. The healthcare provider asks the patient for his/her consent before initiating any transfer so that the resulting transaction occurs directly from one provider to another in accord with patient expectations.

Exchange that involves Data Aggregation, however, must support the process where data is "pulled" from an existing data repository maintained within the HIE

[1] Data and document are used interchangeably in this paper. A document may contain simple text, formatted text, images or structured and vocabulary coded clinical information, or may be made up of a mixture of the above types of content. (IHE, 2012, p. 255)

infrastructure. Data may be subject to secondary disclosure -- the patient's data sharing preferences being stored in a location so that when data is pulled, only those data elements are shared consistent with patient privacy preferences for that type of encounter. Secondary disclosure especially becomes an issue in the case of conflicting or overlapping consents if the patient has been seen by several providers throughout a community and for different reasons. In both cases, the boundary conditions around the data that dictate access are established within the systems where the data was initially collected.

Several key elements govern the exchange of ePHI using an HIE including policies based on regulations, jurisdiction, and organizational practices, data use and sharing agreements, patient privacy considerations and the underlying consent model, and operational procedures.

International and national laws and regulations establish the fundamental basis of policy to regulate the exchange of health-related data, but conflicts and exceptions exist due to local jurisdiction and organizational practices. Within the United States, the HIPAA Privacy Regulation provides a common floor for standard policies and practices governing the sharing of ePHI. But conflicts exist between HIPAA and other federal privacy statues such as 42 CFR that regulates confidentiality around substance abuse. States represent local jurisdictions with often more restrictive requirements than HIPAA in terms of breach reporting and more stringent controls around highly sensitive information, such as HIV/AIDS and mental health (Berkeyheiser et al.; 2008, p. 123). Further exceptions may be defined by the organizational practices of an individual healthcare entity. Especially for HIEs that aggregate information, there is the need to establish a policy and practice framework that harmonizes these often disjoint rules.

Data use and sharing agreements are contracts between HIE operators, data consumers, and data providers that should incorporate all applicable regulatory and exceptions in a uniform manner. Key elements that need to be addressed in such agreements include: data governance (i.e., when is an HIE participant a data owner versus a data custodian versus a data user), standard terms and conditions for exchange (based

on relevant privacy laws), and methods for handling any regulatory or program exceptions to the standard terms and conditions expressed in guiding policy.

Privacy **consents** expressed by an individual patient are commonly used to control the sharing of his/her healthcare information. A provider has a patient sign an **authorization** consenting to the disclosure of his/her records in accordance with the applicable HIE data exchange policy, based on applicable policy. There are a variety of consent models, five of which have become standard in United State since 2010 (Goldstein & Rein, 2010, pp. 5-7):

> **No consent**: The health information of patients under the care of a participating provider organization is automatically included in and available through the exchange, often according to certain rules.
>
> **Opt-out:** A patient is *opted-in* unless he/she *opts out*. All data is automatically available for exchange but with a provision that a patient can opt out in full.
>
> **Opt-out with exceptions:** This is a variation of the opt-out model above. A patient can either opt out in full or 1) selectively exclude categories of data / specific data elements from the exchange, 2) limit exchange of information to specific providers / provider organizations, and/or 3) limit exchange of information for specific purposes.
>
> **Opt-in:** A patient is *opted-out* unless he/she *opts in*. No patient data is automatically made available for electronic exchange unless a patient actively expresses a desire to participate. Like the opt-out model, this option allows for no granularity of patient preference.
>
> **Opt-in with restrictions:** This is a variation of the opt-in model above. A patient must actively grant his/her consent to participate and then has the option to make all of his/her information eligible for exchange or 1) include only specific categories of data or data elements, 2) enable information to flow only to specific providers, and/or 3) allow information to be exchanged only for specific purposes.

Operational procedures are established to ensure uniform operations and compliance with HIE policies. Procedures can address provider training on how to obtain patient consent and authorization, establish guidance on how to comply with the standard rules for disclosure of HIE-governed data, and require a provider acknowledge exceptions to common terms and conditions before ePHI is exchanged in specific cases.

3.2. A Sample Use Case

The following use case scenario illustrates how some of these background elements affect the exchange of information in a HIE network.

Dr. Bob needs to refer his patient, Ted, to a specialist, Dr. Alice. Both Dr. Bob and Dr. Alice are independent providers and both participate in an HIE network that contains a CDR. Dr. Bob will release clinical information about Ted to the HIE that is relevant for the referral. Dr. Alice will retrieve this information from the HIE infrastructure for the purposes of treating Ted.

Dr. Bob reviews the latest copy of the HIE data sharing rules that require he take into account patient preferences regarding the release of address information. He notes from his EHR system that Ted has placed restrictions on disclosure of his physical home address under normal conditions. During the office visit, Dr. Bob informs Ted he will be referring him to Dr. Alice, explains how Ted's information will be shared using the HIE network, and obtains Ted's signature on an HIE patient authorization form. Dr. Bob files the completed HIE patient authorization form in his copy of Ted's record and notes in his EHR system that Ted has opted in to the use of the HIE as of the visit date, provided that his physical home address is not published to the HIE.

Ted signs the Authorization Form confirming that he understands and acknowledges use of the HIE network, consenting to the release of his ePHI in accordance with the applicable data sharing rules (i.e., no physical home address).

Dr. Bob prepares the electronic referral document, drawing on information in Ted's health record needed for the referral. His EHR system, the sending system, assists in ensuring that all applicable data sharing rules applied to the data before release of the information to the HIE network. The HIE network will also provide alerts upon upload.

In this case, both systems will help enforce that the Ted's physical home address must be redacted from the released ePHI. Dr. Bob then publishes the referral to the HIE's CDR for retrieval by Dr. Alice through the HIE provider portal.

Dr. Alice retrieves Ted's information from the CDR using the HIE provider portal as she does not have a certified EHR system. She checks the status of Ted's latest authorization on file with the HIE, including the updates from Dr. Bob. She notes that no physical home address is provided and that her office will have to bill Ted using the post office box address provided.

When Ted arrives for his appointment at Dr. Alice, Emily, the registration clerk at the front desk is smitten. After the appointment, she keeps thinking about him and vows to find out where he lives. Unfortunately, she only has his post office address for billing purposes.

A month later, Ted confronts Emily lurking outside his home. He recognizes her from his appointment with Dr. Alice and he knows that the referral came from Dr. Bob through the HIE network. He files an incident report with the HIE operator.

The HIE operator reviews all activity around Ted's record and confirms that the consent policy was followed according to the authorization that Dr. Bob had Ted sign. The HIE operator also confirms that all access to the referral documents in the CDR is traceable to either Dr. Bob or Dr. Alice since the initial date the referral data was transferred, that no additional documentation has been provided, and that only the appropriate addresses were included. This is corroborated by the system logs on Dr. Bob's EHR system.

In fact, further investigation and correlation of these events with the identity management module in Dr. Bob's EHR system shows that Emily has a close friend that worked in Dr. Bob's clinic as a medical records technician and looked up Ted's home address for Emily as a favor.

3.3. Incident Response and Consent Management

HIE is about the secure exchange of data. Although concern always remains regarding malware and similar attacks, a primary focus is on those breaches that actually

involve the inappropriate access to, handling of, or disclosure of sensitive health data according to privacy rules and concerns, such as shown by the simple scenario above. Incidents can be both intentional (i.e., insider threats such as celebrity snooping, impersonation, modification to cover discovery of fraud) and unintentional (i.e., information routed incorrectly to the wrong person, diagnosis incorrectly coded in the patient record).

Privacy considerations determine the specific business rules related to the confidentiality and release of ePHI. Medical decision making demands the integrity and the availability of clinical information. The two often conflict. Consent management, however, can provide another level of granularity to mitigate these conflicts.

For example, mental health problems are often treated with potent psychotropic drugs that can have deadly implications if not managed properly or if a drug is prescribed for another condition without full knowledge of the patient's current mediation history. Yet, a patient receiving psychotropic medications may have this information normally withheld from his/her primary care physician (PCP) based on the fact that the PCP does not have "a need to know" and could infer the mental health diagnosis from the drugs being listed on the patient's medication history. If the patient provides consent and authorizes his/her PCP to have access, the situation would be mitigated.

So, how can a focus on consent management aid incident response in the case of an HIE-related breach? First, understanding policies can help an incident handler prepare by anticipating the expected behavior around data and better identify an event that could signal a breach of confidentiality. In the above scenario, both the sending system and the HIE network provided Dr. Bob with alerts based on data sharing rules and Ted's patient preferences that actually helped Dr. Bob avoid being guilty of a data breach. Second, correlating consent management with other security related controls, such as data leakage prevention (DLP) and security information event manager (SIEM), have the potential to make identification and containment more proactive, allowing a handler to localize and limit damage to the greatest extent possible. In the scenario, the auditing capability in the HIE network as well as the fact that the HIE logs could be correlated with those of Dr. Bob's EHR system allowed the HIE operator to confirm that the data breach did not

originate from the HIE. Improved analytics and reporting tools can also aid incident analysis, how the incident was related to current policy, and how changes in policy might mitigate future incidents. The HIE operator and Dr. Bob may agree to establish a policy that more closely aligns the IdM capabilities of their respective systems to allow more proactive identification of possible incidents in the future.

4. The Building Blocks – Policies and Standards

Functional requirements represent "the functionality built into the system to satisfy the business requirements" (Wiegers, 2003, p. 6) and sometimes are considered as those requirements that describe the behavior of a system. Non-functional (i.e., technical) requirements represent what a system is – the building blocks of capacity, performance, and standards.

4.1. Functional Requirements and Policies

Policies embody the business rules by which an HIE network operates and can directly influence how the infrastructure is built. Therefore, the policy framework an HIE network will be built on and operated under is part of functional requirements development for its infrastructure. The following table presents those functional requirement categories that will influence the design of a policy-aware HIE network, applicable policy statements, and related procedural areas that will need to be developed to support the detailed requirements and actual policy statements.

Table 1: Requirements, Policy, and Procedures

Requirement Category	Policy Statements	Related Procedural Areas
Access to Data	• Acceptable user authentication methods • Data access rules such as: who (by role) has access to what type of data in the HIE; who (by role) is allowed to publish data into the HIE; assignment of a surrogate for a specific user; elevation of user privileges for emergency or routine operations requiring temporary change in assigned role	• User provisioning/de-provisioning (aka "on-boarding") • Account management • Geo-location services related to user access
Data	• Data classification standards	• ROI, disclosure

Requirement Category	Policy Statements	Related Procedural Areas
Management	• Data acceptance standards for publishing into the HIE (e.g., no mental health information will be accepted) • Rules for release of information (ROI) and disclosure tracking • Rules for secondary disclosure of data aggregated in the HIE • Length of time to maintain data in HIE	accounting, secondary disclosure • Special handling of restricted information
Patient Consent	• Consent model and granularity rules • Rules to override patient specified block (e.g., eminent danger to patient) • Attribute definitions for information release (e.g., explicit to each episode of care, use by specific facilities) • Process to change consent policy for a patient (e.g., change from opt-in to opt-out) • Patient specific rules around ePHI (e.g., allow direct use of shared documents, but no secondary disclosure)	• Consent / Policy Management
Accountability	• Auditing scope and purpose • Trigger events for auditing/ alerting • Geo-location rules for people and records	• Analytics and reporting

HIE policies cannot be isolated from those of participating organizations and should be harmonized across participants in the network if possible. The HIE network states "no data shall be disclosed to a patient's neighbor" as part of its general disclosure policy. Individual participants in the HIE network might define a neighbor as either a person living next door or a person living within 10 miles. A patient might place a further restriction by naming that a specific neighbor (e.g., Emily Jones) cannot view his data. The challenge to the HIE operator will be to aggregate these individual policy statements in order comply with the HIE network's general disclosure policy.

4.2. Technical Requirements and Standards

Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI TF) provides one starting point for HIE technical requirements through a comprehensive family of standard Profiles focused on the details necessary to ensure

interoperability. The IHE Profile most relevant to the implementation of patient consent is the IHE Basic Patient Privacy Consent (BPPC) Profile (IHE, 2012, pp. 174-184). Another key resource is the Data Segmentation Implementation Guidance, published in August 2012 as part of the S&I Framework[2] initiative entitled Data Segmentation for Privacy (S&I Framework, 2012). Both these documents were used in developing the following stack of technologies and standards used to specify the technical requirements.

Table 2: Technical Requirements and Standards (IHE, 2012) (S&I Framework, 2012)

Control	Requirement	Technologies/Standards
Primary Functional Area: Access to Data		
Identification & Authentication	Prove that a system or person is who they say that they are	Personal interactions, Digital Certificates, security assertions, Kerberos, and LDAP
Identity Assertion	Validate identity of requestor to document repository, both for the retrieval of documentation and of the consent	Pull: OASIS SAML Specification v2.0 Push: X.509 Digital Certificate as part of the PKI infrastructure for Direct Messaging
Access	Limit access by an authenticated entity to the information and functions that they are authorized to have access to.	Access Control Model
Transport Mechanism	Required transport and transport security for accessing information	Pull: SOAP header and body Push: SMTP and S/MIME Mobile: REST
Primary Functional Area: Data Management		
Content Structure	Establish the basic structures and formats for data managed by the HIE	HL7 specification for Consolidated Clinical Document Architecture (CDA)
Content Tagging	Establishes static metadata (i.e., Confidentiality Code) within data that is used to determine how to handle the disposition of the data	CDA R2 (Header, Section, Entry)
Confidentiality	Protect sensitive information from exposure when created, stored, communicated, and/or modified	Encryption, access controls, DLP Mutually authenticated TLS v1.0 or greater
Data Integrity	Data has not been changed in	Digital signatures, secure hash

[2] The S&I Framework is an on-line forum supported by ONC's Office of Standards & Interoperability to allow industry stakeholders to solve real-world interoperability issues in health information technology. It is located at http://wiki.siframework.org.

Control	Requirement	Technologies/Standards
	an unauthorized way	algorithms, CRC, and checksum
Functional Area: Consent/Policy Management		
Patient Privacy	Enforce patient specific handling instructions	Consent model, consent management, data classification techniques
Policy/Consent Metadata	Attributes associated with a policy such as handling for privacy and security, provenance, patient information, and consent	IHE Profiles: Cross-Enterprise Document Sharing (XDS); Cross-Enterprise Document Reliable Messaging (XDR); Cross-Enterprise Document Exchange on Media (XDM); Cross-Enterprise User Assertion (XUA) HL7 CDA Consent Directive DSTU Metadata
Primary Functional Area: Accountability		
Accountability	Prove the system is protecting the resources in accordance to the policies.	Audit logging, reporting, alerting, alarming IHE Audit Trail and Node Authentication (ATNA) IHE Consistent Time ASTM E2147
Non-Repudiation	Ensure that an entity cannot later refute that they participated in an act	IHE Document Digital Signatures.

4.3. Focus on Incident Response

The SANS Institute identifies six steps to handling an incident most effectively (SANS Institute, 2010, p. 14.). Reviewing how the functional and technical requirements above could support proactive incident response and handling suggests additional requirements that are more implementation oriented.

Table 3: Incident Response and Handling Requirements

Step	Need	Requirement
Preparation	Understand policies related to data access, including an understanding of how data attributes affect HIE network rules of behavior	Centralize consent/policy administration Develop ability to simulate the application of a specific policy or set of policies to data and evaluate the resulting behavior
Identification	Identify and contain incidents in real time (or near real time)	Provide capability to correlate HIE activity logs with IdM events

Step	Need	Requirement
Containment	Determine extent of a given breach of information across HIE network and all participating systems that might be affected	Centralize consent/policy application (i.e., establish policy-based blocks on for access to specific data in the HIE) Correlate logs with other edge systems that participate in the HIE (i.e., EHR systems)
Eradication	Provide assurance that problem is corrected and any breached data recovered or removed	Implement an acceptable proof-of-storage approach that allows validation that breached data has been recovered or removed.
Lessons Learned	Provide after-action report	Provide in-depth analytics that support lessons learned Develop ability to simulate a previous incident and review for improvements to established best practices

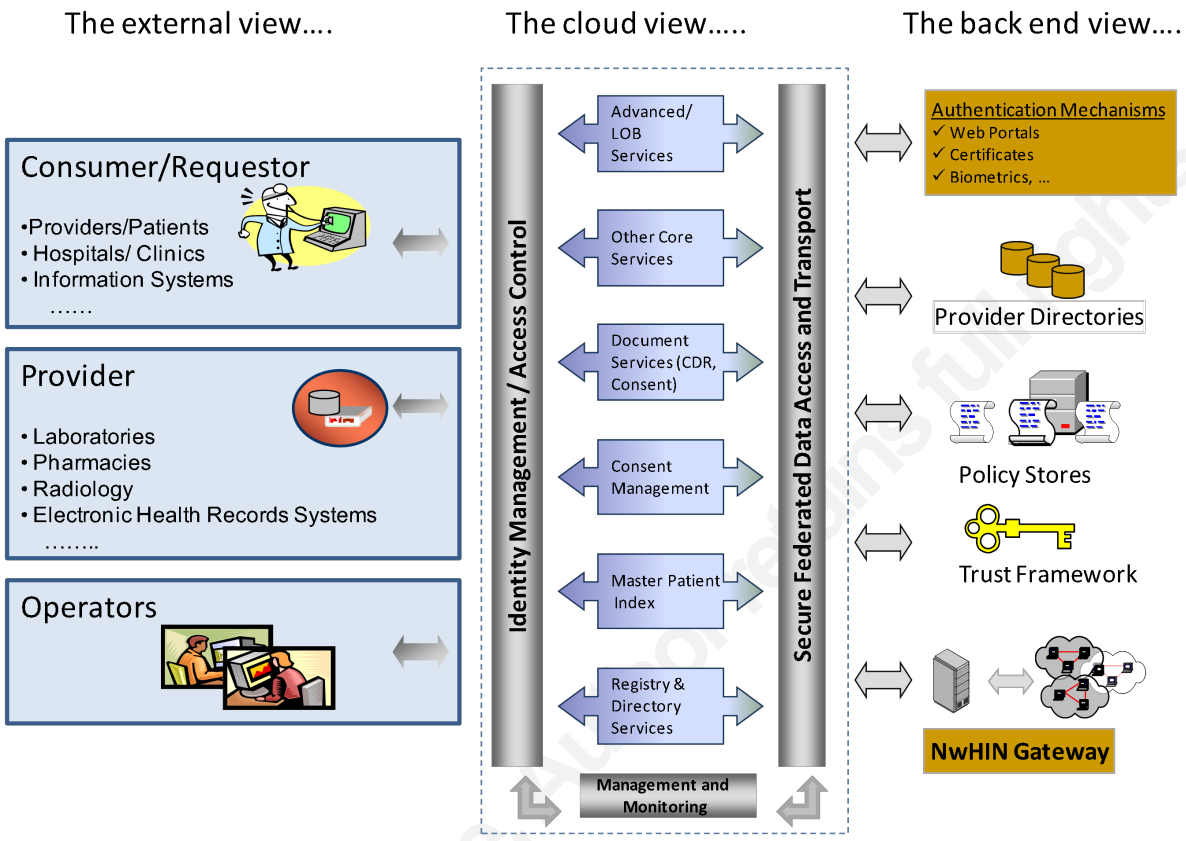
5. Policy-Based Reference Architecture

This section first presents relevant concepts around a cloud-based HIE infrastructure and then outlines a reference architecture from which system requirements, the "the top-level requirements for a product that contains multiple subsystems" (Wiegers, 2003, p.7) and a more detailed implementation specification can eventually be created.

5.1. Cloud-Based HIE Infrastructure

Figure 1 represents a cloud-based HIE infrastructure based on a service-oriented architecture (SOA), illustrating the three basic views needed to understand how a policy- and consent-based reference architecture for HIE can come together.

Figure 1: HIE Infrastructure



The **external view** is shared by consumers, providers, and operators according to the rules established by the HIE network for identity management and access control.

Consumers or **requestors** of information from the HIE network include both individual healthcare professionals and organizations, such as private hospitals, long term care facilities, ambulatory clinics, and public health agencies. HIE access can be established through a user's EHR system, via a provider portal, or mobile devices such as a tablet or smart phones.

Providers of data and services to the HIE include those entities that provide ancillary services and data such as laboratories, pharmacies, and radiology associates. EHR systems managed by hospitals, clinics, and individual providers also provide data to the HIE.

Operators are responsible for the administration, management and monitoring of the HIE network and its information.

Barbara Filkins, filkins@impulse.net

Next, the **cloud view** is comprised of several key services, not all of which need to be functional in a HIE network depending on whether the HIE is engaged in purely Directed Exchange[3], Data Aggregation, or both. Key HIE services include:

- **Security Services,** noted by the grey bars in Figure 1, include identity management (IdM) and access control, secure data access and transport across domain boundaries, and management and monitoring of HIE network activities, including the movement of data. Some level of security and privacy duties are pushed to those HIE-edge systems operated by the participating organizations. These systems may include organizational provider directories, EHR systems, laboratory information management systems (LIMS), pharmacy systems, and other repositories of patient information like disease or immunization registries.
- **Registry and Directory Services** brings together the identities, roles and access control credentials necessary to support access to the HIE network and draws from the IdM systems and provider directories at participating entities.
- **Master Patient Index (MPI)** is the service used to correlate patients and their data across multiple data repositories, an activity essential to many HIE functions as patient records are typically held in multiple locations. An MPI matches various information elements known to be related to a specific person across multiple patient records. Various MPIs use different algorithms. While close, none can achieve 100% accuracy (Kolkman and Brown, 2011, pp. 154-155).
- **Consent Management** is required to specify what permissions have been granted by patients, within allowable limits specified by each participating organization and the applicable jurisdictions. Patient consent may require fine gained access control based on the consent model chosen.
- **Document Services** includes a repository for data and documents and capabilities for managing, locating, and retrieving the information in HIE repositories. A specific instance of Document Services is the CDR where data

[3] A HIE that provides just Directed Exchange is called a Health Information Service Provider or HISP.

is consolidated from various HIE clinical participants to present a unified view of a single patient.

- **Other Shared Services** are those that are normally available to participants in an HIE network. Typical examples include terminology and transformation services which offer standardization across the terms and code used by participants and record locator services that point to those locations where authorized information can be found about a patient.
- **Line of Business (LOB) Services** are specific to the needs of the community connecting to an HIE network. Examples might include clinical results delivery for laboratory or diagnostic results, public health reporting, or limited EHR capability for a provider who does not have his/her own system.

Finally, the **backend view** consists of infrastructure elements that must be coordinated for an HIE network to provide enterprise-level services across a number of otherwise unaffiliated entities. Harmonization of authentication and protection methods, provider directories, and policies are all critical to successful governance and operation.

5.2. Towards a Policy-Aware Architecture

The concept of a consent- or policy-aware HIE infrastructure to enable control around sensitive data is underscored by several key areas that must converge -- data governance policies, identity management, more granular access control models, proactive approaches to data leakage or loss, and identity activity management.

Data governance policies are written to enforce desired behavior around the sharing of sensitive data. Translation of these policies into an executable, coded structure allows attributes inherent in the electronic data to trigger policy rules and control the enforcement of these policies in a virtual space. This is an example of a rules-based information system common in healthcare for claims processing, benefits eligibility determination, and clinical decision support.

The eXtensible Access Control Markup Language (XACML), based upon XML is a way to specify access control policy in a machine-readable format. Patient consents, expressed as active XACML policies, are brought together at a specific point in the HIE

network with other critical information to make an access control decision. A static 'confidentiality code' embedded in the data published to the HIE triggers dynamic rules that apply the consent rules to the data and determine the appropriateness of its release. Alignment of these policies with the basic vocabularies around consent management being developed by various healthcare standards bodies is an important consideration for implementation.

Identity management remains a central concern for healthcare data governance. IdM parameters, such as user role and related permissions, are critical attributes in making access control decisions. IdM technology and methods provide the foundation for an effective patient consent management system. A patient consent may itself represent a sensitive document so the identity of the person requesting access to the consent also needs to be verified (typically via a SAML assertion). Additional identity verification on the patient may also be required so the MPI may be called on to provide additional attributes as well.

The healthcare industry is moving to **more granular access control models**. The current emphasis on role-based access control (RBAC) began with the minimum necessary standard in the HIPAA privacy rule that "requires covered entities to make reasonable efforts to limit protected health information (PHI) to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request" (Amatayakul, Brandt, & Dennis, 2002). A role is a grouping of individuals with similar permissions (i.e., the right to do something) and more complex roles can be achieved by combining simpler ones. Attribute Based Access Control (ABAC) is another model gaining in popularity. ABAC is a more advanced "access control model wherein the access control decisions are made based on a set of characteristics, or attributes, associated with the requester, the environment, and/or the resource itself" (NIST, 2009, p. 5).

However, both these models have limitations in an HIE environment where the approach to access control should be harmonized across all participants. RBAC is limited in being able to differentiate individual members of a role/group to selectively allow or deny access based on a granular set of attributes for each person. Administrators at HIE network participants may be mapped to the same role in the HIE but may represent vastly

different levels of access to data, such as for a large hospital versus a small clinic, resulting in more numerous versions of the HIE administrator role (or workarounds) that become unwieldy to manage (NIST, 2009, p. 5). Similarly, ABAC is a local access control model. ABAC attributes, such as allowable user credentials, may be consistent across each HIE participating organization, but may vary widely from one participant to another.

A potential solution, still considered an emerging technology, is Policy-based Access Control (PBAC), "an emerging model that seeks to help enterprises address the need to implement concrete access controls based on abstract policy and governance requirements" (NIST, 2009, p. 7). PBAC is considered "a harmonization and standardization of the ABAC model at an enterprise level in support of specific governance objectives" (NIST, 2009, p. 7) and thus addresses the challenges faced by an HIE operator to develop consistent policies across the HIE network. As does ABAC, PBAC combines attributes associated with the requester, the environment, and the resource but then applies those attributes using an additional set of rules established by the HIE network that are related to the circumstances under which the request is made..

Another place where enforcement of policy, including patient consent, is critical is at that porous boundary between a user and cloud-based content where **data loss or leakage** easily can occur Content-aware DLP technology can provide a policy-based sieve through which data passes between two parties as well as help enforce that policy in a nontransparent mode that can affect (and hopefully correct) user behavior before an incident would actually occur.

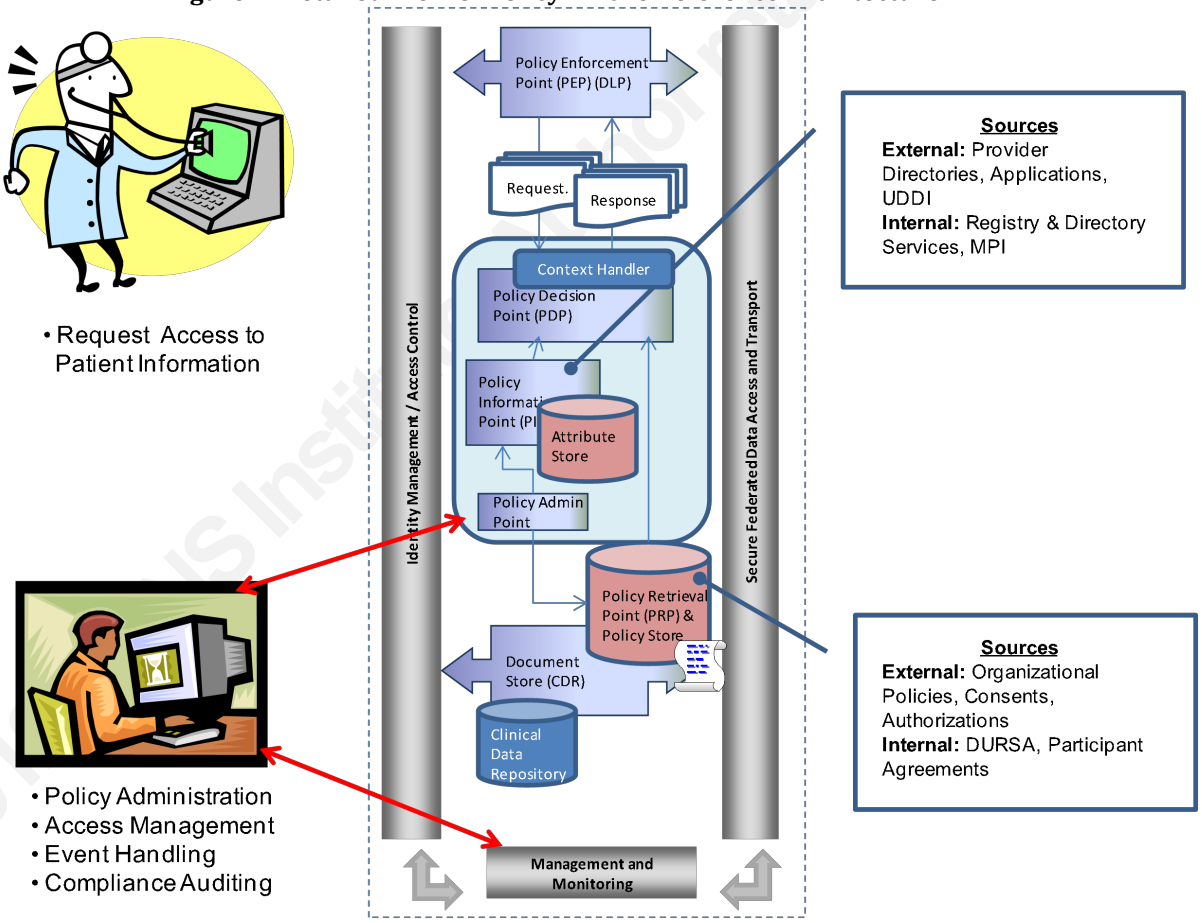
Incident response is difficult enough when the challenge is simply trying to understand what happened on the network by gathering information from a collection of network and security devices, diligently piecing a set of "thin events" together using various logs. However, tools such as SIEMs, can tie user identity and other related information to event logs (Northcutt, 2009). Taking this a step further, correlating these events with the HIE IdM capabilities could allow the HIE operator to establish **identity activity monitoring** as part of an overall auditing and logging strategy. This would correlate specific activities around sensitive data to specific, identified users or systems,

allowing the HIE operator to tie those changes to what would be expected if the user was working with the data in accordance with established policy.

5.3. Assembling the Pieces

The OASIS XACML 2.0 Core specification allows for an elegant, efficient, and modular reference architecture whose design and implementation correlate well with key components within an HIE infrastructure (Moses, 2005, pp. 16-18). A reference architecture based on this standard is shown in Figure 2 and described below, based closely on the description in the OASIS specification document (Moses, 2005, pp. 16-18).

Figure 2: Detailed View of Policy-Aware Reference Architecture



The **Policy Administration Point (PAP)** is where policies and policy sets are written (e.g., transcribed from written policies to machine-oriented versions) and made

available to the consent management service. The PAP should provide (a) an interface to manage policies and their lifecycle, (b) a client (XACML-aware) to facilitate the policy-authoring task, and (c) the ability to simulate the application of a policy or policy set to data and evaluate the resulting behavior. Potentially, the PAP could be a stand-alone application for policy development, simulation, and evaluation. The PAP should interface to the IdM system to be able to include IdM policies in support of policy development and simulation.

Some, but not all renditions of XACML architectures, include a **Policy Retrieval Point (PRP)**, through which policies are read from a repository. Within the HIE, the PRP for consent and other policy management may be considered part of HIE Document Services. The design of the PRP should ensure the independence from specific storage mechanisms.

When a user requests access to clinical documents or data for a specific patient being held in the HIE's CDR, this request is intercepted and acted upon by the **Policy Enforcement Point (PEP)**. A PEP may be implemented as native to an HIE-edge device or application accessing the HIE. A PEP could be implemented with DLP technology/products through which all data access requests from external users are managed, enforcing both access policy and acceptable user behavior.

The PEP then sends the request for data access, including any attributes germane to the present user session or service request, to a **context handler**. The context handler intercepts the request, converts it from the native form of the originating device or application into XACML, and draws in additional attributes from the **Policy Information Point (PIP)**.

A PIP is an attribute store, located anywhere in the network. Attributes (e.g., descriptions of users, services, resources, actions, and the environment) can include a user's name, their role in an organization, the types of information they can access, the patients they can access, and the time of day. Sources for attributes can be external to the HIE such as organizational provider directories, legacy applications, and UDDI discovery points and internal to the HIE such as the MPI.

Once attributes have been obtained, the context handler sends the XACML request to the **Policy Decision Point (PDP)** – the functional heart of this architecture. The PDP identifies the applicable policy or policy set, retrieves the required attributes from the context handler, evaluates the policy or policy set together with the retrieved attributes, and reaches a decision as to authorization or access. It then returns the response context (including the authorization decision) to the context handler.

The context handler translates the response context back to the native response format of the PEP and returns the response to the PEP. The PEP fulfills the obligations of the request, handling its fulfillment according to the PDP decision – granting access to the data if the decision was *permit*, denying access if otherwise.

6. Findings and the Future

Data governance for ePHI will become more complex with the emergence of personal health records, contention over ownership of clinical data and what is being done with it when accessed, (Dolan, 2011) and the increased value of clinical information combined with an individual's financial history, an open door to medical identity theft.

The adoption of cloud computing alters the very fabric of traditional computing. Infrastructure concerns essentially drop away as explicit organizational control over the physical infrastructure is outsourced. Incident response must increasingly focus on the actual data and virtual enforcement of policies. Response processes become more challenging as the cloud offers new questions – how can one make sure that their sensitive data was really deleted from a cloud-based repository? New tools and techniques will definitely be needed, backed by shared legal and financial responsibility if policies are not followed.

To support this new paradigm, functional and technical requirements have been identified for the use of policy-based access control built around policy and consent management in a cloud-based HIE. A reference architecture has also developed.

Key considerations include:

- HIEs, especially those that aggregate data, need IdM systems built on policy-based access control models as current role-based models may become too complex to manage and simpler attribute-based models may lack scalable consistency across unaffiliated HIE participants.
- The OASIS XACML specification suggests a modular architecture with components that can be mapped to both existing HIE network functions and security technologies, although this will require a systems integration approach for fulfillment.
- XACML can provide a policy definition structure and the vocabulary should be consistent with efforts currently underway by various standards bodies, including S&I Framework. HIE policies will also need to be aligned with those policies provided by the edge systems (e.g., the participating EHR systems), resulting in a continuing emphasis on semantic interoperability.
- DLP tools should be incorporated into the infrastructure as policy enforcement points, working in conjunction with IdM and consent management services, to ensure compliance with policy through affecting and correcting user behavior before an event or incident involving sensitive data actually occurs.
- Incident response around events involving sensitive data routed and managed by an HIE should be proactive, rather than reactive. Integration of SIEM tools with IdM systems and policy- and consent-based access can create a policy-aware infrastructure that will build on the starting point represented by the *syslog*-based IHE ATNA Profile (IHE, 2012, p. 69).
- Identity activity management should be incorporated into the managing and monitoring functions of HIE networks as a future strategy.

Table 4 provides a high-level traceability matrix relating the functional and technical requirements in Table 2 and Table 3 to the key components of the reference architecture. The next step should be to develop a complete set of system requirements followed by a detailed design for each component, whether based on custom software

development or identification of commercial products, eventually integrating these components in an overall HIE infrastructure concept and network design.

Table 4: Traceability Matrix

Requirement Reference			Architecture Component
Functional	**Technical**	**Incident Response**	
Access to Data	Identification & Authorization Identity Assertion Access Control Transport Mechanism	Centralize consent/policy administration Provide simulation and evaluation capability	Policy Administration Point Identity Management System • Authentication • Authorization • Audit
Data Management	Content Structure Content Tagging Confidentiality Data Integrity	Centralize consent/policy application Implement an acceptable proof-of-storage approach that allows validation that breached data has been recovered or removed.	Policy Enforcement Point Data Leakage Protection • Policy/content based • At data element level • At the document level • At the message level Document Store/CDR Policy Retrieval Point & Policy Store
Patient Privacy	Patient Privacy Manifest Metadata	Centralize policy/consent administration and application	Consent Management Service Context Handler Policy Information Point Policy Decision Point
Accountability	Auditing Non-repudiation	Provide capability to correlate HIE activity logs with IdM events Correlate logs with other edge systems that participate in the HIE Provide in-depth analytics that support lessons learned	SIEM Log Management Analytics

7. References

1. American Health Information Management Association (AHIMA). (n.d.). *Health Information Exchange*. Retrieved from: http://www.ahima.org/resources/hie.aspx.
2. Amatayakul, M., Brandt, M. D., & Dennis, J. C. (2002). Implementing the minimum necessary standard (AHIMA Practice Brief). *Journal of AHIMA,* 73(9), 96A-F. Retrieved from: http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_015785.hcsp?dDocName=bok1_015785.
3. Berkeyheiser, L., Brock, C., Gensinger, R., Miller, J., Sivek, A., Schulte, M.F., & Williams, M. (2008). *Preparing for Success in Healthcare Information and Management Systems: The CPHIMS Review Guide.* Chicago, IL: Health Information and Management Systems Society (HIMSS).
4. Dolan, P. L. (2011, July 4). AMA to draft model legislation on information exchanges. *American Medical News.* Retrieved from: http://www.ama-assn.org/amednews/2011/07/04/prsl0704.htm.
5. Goldstein, M. M. & Rein, A. L. (2010*). Consumer consent options for electronic health information exchange: policy considerations and analysis, prepared for Office of Policy and Planning, Office of the National Coordinator for Health IT*. Retrieved from: http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11673_911197_0_0_18/ChoiceModelFinal032610.pdf
6. Integrating the Healthcare Enterprise (IHE). (2012). *IHE IT Infrastructure (ITI) Technical Framework Volume 1 (ITI TF-1) Integration Profiles Revision 9.0 – Final Text.* Retrieved from: http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_Vol1.pdf
7. Kolkman, L. & Brown, B. (2011). *The Health Information Exchange Formation Guide.* Chicago, IL: Healthcare Information and Management Society (HIMSS).
8. Moses, T. (ed.). (2005). *eXtensible Access Control Markup Language (XACML) Version 2.0 Specification Document.* Retrieved from: http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf.
9. National Institute of Standards and Technology (NIST). (2009). *A Survey of Access Control Models.* Retrieved from: http://csrc.nist.gov/news_events/privilege-management-workshop/PvM-Model-Survey-Aug26-2009.pdf
10. Northcutt, S. (2009, April). Tying log management and identity management shortens incident response [Web blog post]. Retrieved from: http://searchsecurity.techtarget.com/magazineContent/Tying-log-management-and-identity-management-shortens-incident-response
11. Office of the National Coordinator (ONC) for Health IT. (2012). *Privacy and Security Framework Requirements and Guidance for the State Health Information Exchange Cooperative Agreement Program* (Document No. ONC-HIE-PIN-003). Retrieved from http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_0_5545_1488_17157_43/http%3B/wci-

Barbara Filkins, filkins@impulse.net

pubcontent/publish/onc/public_communities/_content/files/onc_hie_pin_003_final.pdf
12. Ponemon Institute. (2011). *Second Annual Benchmark Study on Patient Privacy & Data Security.* Retrieved from: http://www2.idexpertscorp.com/assets/uploads/PDFs/2011_Ponemon_ID_Experts_Study.pdf
13. Rouse, M. (2012, September 22). Definition of incident response [Web blog post]. Retrieved from http://searchsecurity.techtarget.com/definition/incident-response.
14. S&I Framework., U.S. Health and Human Services Office of the National Coordinator for Health IT. (2012). *Data Segmentation Implementation Guidance, Version 1.0.3, Consensus Review.* Retrieved from: http://wiki.siframework.org/file/view/Data+Segmentation+for+Privacy+Implementation+Guidance_consensus_v1_0_3_Final.pdf
15. The SANS Institute. (2010). *Incident Handling Step by Step and Computer Crime Investigation.* (Vol. 504.2). Bethesda, MD: The SANS Institute.
16. Wiegers, K. E. (2003). *The Essential Software Requirement*. Redmond, WA: Microsoft Press.

Barbara Filkins, filkins@impulse.net