Integrating the Healthcare Enterprise

IHE IT Infrastructure White Paper HIE Security and Privacy through IHE Profiles

Version 2.0

August 22, 2008

Table of Contents

1 Introduction

Regions and Nations around the globe are looking to link healthcare practices together into Health Information Exchanges (HIE). A Healthcare Information Exchange (HIE) is a set of healthcare entities that are cooperating to share healthcare information about common patients. The Integrating the Healthcare Enterprise (IHE) has proposed a basic method of providing a HIE through an infrastructure that allows for the sharing of clinical documents about a patient in a way that allows for long term use. The interoperability necessary for such an infrastructure is based on a comprehensive family of Profiles centered on the Cross-Enterprise Document Sharing (XDS) Profile. This white paper will discuss how an HIE that leverages IHE Profiles can protect patient privacy and information security.

The organizers of an HIE need to implement basic security principals in order to offer a security model that protects the HIE - information exchanges. One key element of the interoperability solution put forth by IHE is to share discrete information in the form of documents. These source attested documents may be simple text documents, formatted documents using standards such as PDF, or fully structured and coded using standards such as HL7 CDA. These documents are shared with reference to the individual patient with the expectation that in the future they can be used to provide better healthcare treatment to that same individual patient. This XDS infrastructure is not the only way to implement a HIE, but will be used in this white paper as the IHE security and privacy model.

A very important aspect that is beyond the scope of IHE is the definition of the overall Policies of the HIE. There is guidance in the IHE Technical Framework, but there is no single policy that must be put in place by an IHE based HIE to ensure privacy and security. In this white paper we will discuss potential policy decisions and positions with regard to the profiles. It is very important for the reader to understand that the scope of an IHE profile is only the technical details necessary to ensure interoperability. It is up to any organization creating an HIE to understand and carefully implement the policies of that HIE and to perform the appropriate risk analysis. Although this white paper is not going to define the policies that an HIE should have, we are going to explore some of the policy building to demonstrate how such policies can be supported.

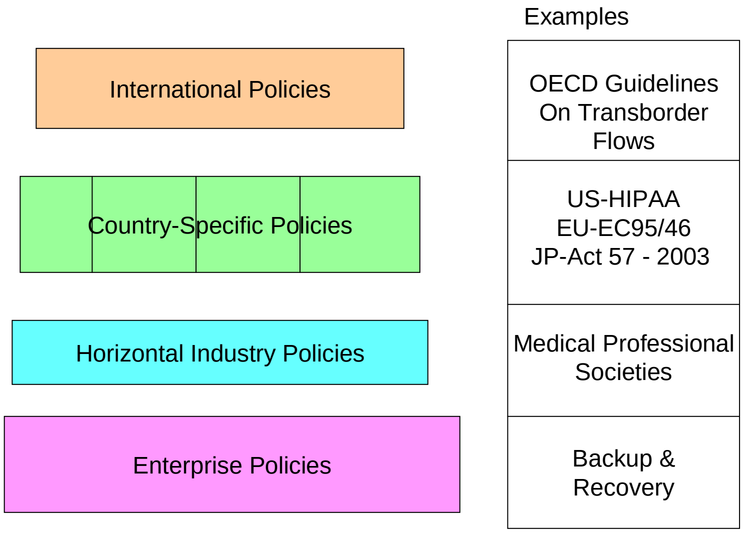
Examples
International Policies
OECD Guidelines On Transborder Flows
Country-Specific Policies
US-HIPAA
EU-EC95/46
JP-Act 57 - 2003
Horizontal Industry Policies
Medical Professional Societies
Enterprise Policies
Backup & Recovery

Figure 1: Policy Environment

The Policy Environment is made up of many layers of policies as shown in Figure 1. These policies work together in a hierarchic way to interlock. We will introduce some of these layers in this white paper and show how they influence the technology. At the highest layer are international policies, like the International Data Protection Principles. Countries or regions will have specific policies. Some examples are USA HIPAA Security and Privacy Rules, with further refinement by the states. There are horizontal policies that are common among a specific industry, such as those from medical professional societies. Then within the enterprise will be specific information technology policies. As shown in this white paper, the IHE Profiles offer not only the means to exchange information, but to do so in a way that is supportive of many of the policies mentioned.

2 Scoping Security and Privacy

The policy landscape that the HIE is built on needs to be defined well before we can build an HIE.

2.1 International Data Protection Principles

In 1980, the Organization for Economic Cooperation and Development ("OECD") developed Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. These guidelines were intended to harmonize national privacy laws, uphold human rights, and promote the free flow of information among its 30 member countries. The OECD guidelines have served as a basis for data protection laws in the United States, Europe, Canada, Japan, Australia, and elsewhere. Together, these principles and laws provide a useful framework for developing general data protection requirements for health information systems.

These OECD data protection principles will be discussed below. The technical controls that are relevant to an IHE HIE are distilled below.

2.2 Policies and Risk Management

IHE solves Interoperability problems via the implementation of technology standards. It does not ***define*** Privacy or Security Policies, Risk Management, Healthcare Application Functionality, Operating System Functionality, Physical Controls, or even general Network Controls.

While HIE Policies and Risk Management are outside its scope, IHE does recognize that these elements are a necessary piece of a system implementation. IHE IT Infrastructure technical white paper, "Template for XDS Affinity Domain Deployment Planning" outlines some of the issues that should be evaluated to be included in the local Policy creation and Risk Management decisions. Also, the IHE IT Infrastructure Planning Committee has produced a white paper that guides IHE profile developers on detail risk identification so the profiles can properly advise system implementers. It is therefore the duty of system implementers to take this guidance into account as part of their Risk Management practices.

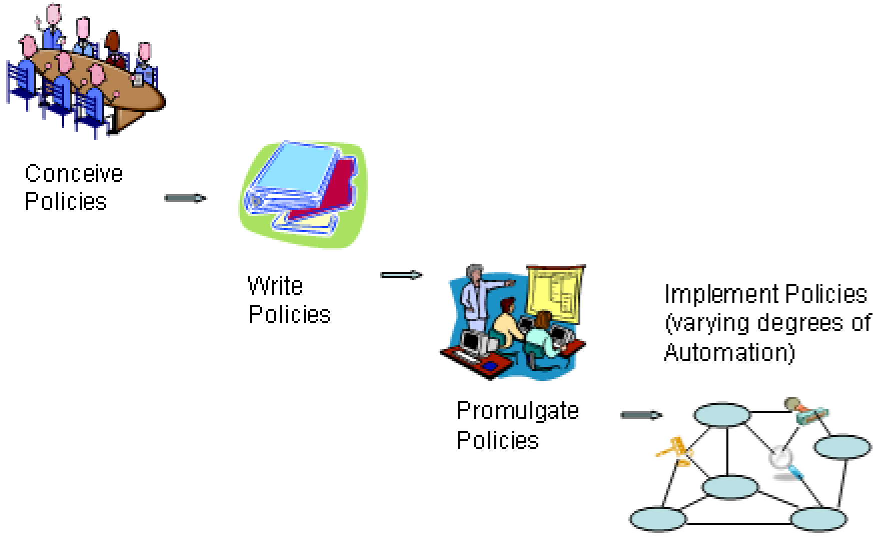

Figure 2: Policy Lifecycle

Figure 2 shows how the corporate Polices are developed, promulgated, and eventually implemented with varying degrees of automation. Policy enforcement must be a part of this policy lifecycle.

HIE implementers need to be aware of different kinds of policies that need to be harmonized with those policies of the local health enterprises connected to the HIE. The following is a list of sample policy fragments to stimulate discussion:

a. Policies for who has access to what type of documents in the HIE
b. Policies for who is allowed to publish documents into the HIE
c. Policies on the acceptable types of documents that can be published into the HIE
d. Policies that indicate acceptable levels of risk within HIE
e. Policies that indicate what sanctions will be imposed on individuals that violate the HIE policies
f. Policies on training and awareness
g. Policies on user provisioning and de-provisioning within the HIE and local operation
h. Policies on emergency mode operations
i. Policies on acceptable network use (browser, decency, external-email access, etc)
j. Policies on user authentication methods that are acceptable
k. Policies on backup and recovery planning
l. Policies on acceptable third party access

m. Policies on secondary use of the information in the HIE
n. Policies on the availability of the HIE (is the HIE considered life critical, normal, or low priority)
o. Policies for maintenance downtime
p. Policies for length of time that information will be maintained in the HIE

These policies are not a flat set, but often interlock and at other times cascade. A good example of this is the cascade of policies related to access to a patient's data. At the Community level, there could be a Policy with general goals indicating that data is not to be disclosed to a person's neighbor. This is further refined at the Enterprise Policy where a 'neighbor' would be defined given the known population and social norms. This Policy can further be refined by the patient themselves in their own privacy consent where specifically a hostile neighbor might be named.

An important set of policies are those around emergency modes. There are wide definitions of cases that are often referred to as emergency mode. These emergency modes need to be recognized for the risks they present. When these use cases are factored in up-front, the mitigations are reasonable.

- Natural or man made catastrophic disaster (e.g. Hurricane, Earth Quake) – often times additional workforce migrates into the area from other places to help out. These individuals need to quickly be screened and provisioned with appropriate access.
- Utility failure (e.g. electric failure) – this situation is common and easily handled through uninterruptible power supplies and backup generation
- IT infrastructure failure (e.g. hard drive crash) – this situation is also common and handled through common infrastructural redundancy
- Need to elevate privileges due to a patient emergency, often called break-glass (e.g. nurse needs to prescribe)
- Need to override a patient specified block due to eminent danger to that patient – this override is not a breaking of the policy but is an explicit condition within the policy.

Often times being in the emergency department is considered as an emergency mode, but the emergency department is really a normal mode for those scheduled to work there. When looked at as normal mode, the proper privileges and workflow flexibility can be specified.

Policy development often is frustrated by apparent conflicts in policies. These conflicts are often only on the surface and can be addressed upfront once the details of the policy are understood. For example in Europe there are policies that forbid the recording of race, yet this is an important clinical attribute. This superficial conflict might be addressed by recording genetic markers instead of race. Another good example of a policy conflict is in records retention requirements at the national level vs at the Medical Records level. Medical Records regulatory retention is typically fixed at a short period after death, yet if the patient has black lung then the records must be preserved well beyond.

2.3 Technical Security and Privacy controls

Based on the experience of the IHE participants in implementing HIE environments there is a common set of Security and Privacy controls that have been identified. These controls are informed by a combination of the OECD data protection principles, experience with explicit policies at HIE implementations, and Security Risk Management.

These security and privacy controls are:

1) Accountability Controls – The controls that can prove the system is protecting the resources in accordance to the policies. This set of controls includes security audit logging, reporting, alerting and alarming.
2) Identification and Authentication Controls – The controls that prove that a system or person is who they say that they are. For example: personal interactions, Digital Certificates, security assertions, Kerberos, and LDAP.
3) Access Controls – The controls that limit access by an authenticated entity to the information and functions that they are authorized to have access to. These controls are often implemented using Role Based Access Controls.
4) Confidentiality Controls– As sensitive information is created, stored, communicated, and modified; this control protects the information from being exposed. For example: encryption or access controls.
5) Data Integrity Controls – The controls that prove that the data has not changed in an unauthorized way. For example: digital signatures, secure hash algorithms, CRC, and checksum.
6) Non-Repudiation Controls – The controls that ensure that an entity can not later refute that they participated in an act. For example author of a document, order of a test, prescribe of medications.
7) Patient Privacy Controls – The controls that enforce patient specific handling instructions.
8) Availability Controls – The controls that ensure that information is available when needed. For example: backup, replication, fault tolerance, RAID, trusted recovery, uninterruptible power supplies, etc.

To show how the above security and privacy controls support the OECD data protection principals we will examine two of the OECD data protection principals: Security Safeguards and Accountability. This can be viewed as:

Security Safeguards:

- I want to be sure the data are not disclosed to someone who shouldn't see them
  - Identification and Authentication Controls.
  - Access Controls.
  - Confidentiality Controls.
  - Patient Privacy Controls.
- I want to be sure the data are not modified by someone who doesn't have the right for that
  - Identification and Authentication Controls.
  - Access Controls.
  - Data Integrity Controls.
  - I want to be sure the data can be retrieved when needed

  - Availability Controls
  - Accountability:
- I want to be sure who is doing action
  - Identification and Authentication Controls.
- I want to know what is done by whom
  - Accountability Controls.
- I want to be sure what has been done cannot be denied
  - Non-Repudiation Controls

These security and privacy controls are not useful without input from the various types of policies that reflect any individual environment and expectation. We will assume a conservative set of policies and show how these controls can be applied when systems communicate on the basis of the IHE Profiles.

Having depicted the range of security and privacy controls generally applicable to the health information shared within an HIE, the next section provides an overview on the way IHE Profiles may be used to support these controls.

3 Applying Security and Privacy to an HIE

IHE does not set policies but is policy sensitive. Therefore we now discuss the policy enabling technologies and not the policies themselves.

This section shows how the existing security controls in the local health IT system are leveraged and extended when they become interconnected into an HIE.

3.1 Patient Privacy Consent to participate in an HIE

Privacy Consents expressed by the patient are commonly used to allow control of shared information in an HIE.. There are many models that offer the patient different types of controls. IHE has published the Basic Patient Privacy Consents (BPPC) Profile that can be used to enable basic privacy consent controls. At this time the standards are under development by organizations such as OASIS, HL7, ISO, ASTM, and others. When these standards are complete patient privacy consents will be more comprehensive and allow the patient to exert far more complex controls than are possible with BPPC. That said, BPPC still provides a rather extensive but coarsegrained level of controls, which may be sufficient in many cases. Some examples of the type of policy that can be enabled by BPPC are:

- Explicit Opt-In (patient elects to have some information shared) is required which enables HIE allowed document use
- Explicit Opt-Out (patient elects to not have information shared) stops all document use
- Implicit Opt-In allows for document use
- Explicit Opt-Out of any document publication
- Explicit Opt-Out of sharing outside of use in local care events, but does allow emergency override
- Explicit Opt-Out of sharing outside of use in local care events, but without emergency override
- Explicit authorization captured that allows specific research project
- Change the consent policy (change from opt-in to opt-out)
- Allow direct use of shared documents, but not allowed to re-publish
- Enable use of document retrieval across communities using IHE Cross-Communitay Access Profile (XCA)
- Explicit individual policy for opt-in at each episode of care event
- Explicit policy enabling the use of the data at a specified facility

The BPPC profile can be used as a gate-keeper to the HIE. BPPC does not define the policies, but does allow for a HIE that has defined its set of policies to capture that a patient has choosen one or more of those policies.

For example: Let's say that the above set of sample policy fragments was available to a patient in a HIE. The patient could agree to Opt-In, and also agree to cross-community access, and also agree to a specific research project. This set of acknolwgements would be captured as one or more BPPC documents. These documents would indicate the policy that is being acknowledged, the date it is being acknowledged, an expiration date if applicable, etc. Then the systems involved in the HIE can know that the patient has acknowledged these policies and thus the patient's choices can be enforced. A system that is doing research can see that this patient has acknowledged participation in the research project, while other patients have not.

Let's further examine what happens when the patient changes their decision. For example, the patient is moving to a totally different region that is not served by this HIE. The patient can acknowledge the Opt-Out policy. This policy would then be registered as a replacement for the previous Opt-In policies including the research policy. Thus now if that research application tries to access the patient's data, it will be blocked as the patient does not have a current acknowledgement of the research policy.

3.2 Protecting different types of documents

XDS allows for many different types of documents to be published for sharing. These documents are likely to have different levels of confidential information in them. For instance, one document might contain the very basic health information that the patient considers widely distributable. Another document might be made up totally of information necessary for proper billing such as insurance carrier and billing address. Yet another document might carry the results of a very private procedure that the patient wishes to be available only to direct care providers. This differentiation of the types of data can be represented using a diagram like found in Table P-1: Sample Access Control Policies (duplicated from the IHE ITI Technical Framework).

Sensitivity **Functional Role**	**Billing Information**	**Administrative Information**	**Dietary Restrictions**	**General Clinical Information**	**Sensitive Clinical Information**	**Research Information**	**Mediated by Direct Care Provider**
Administrative Staff	X	X					
Dietary Staff		X	X				
General Care Provider		X	X	X			
Direct Care Provider		X	X	X	X		X
Emergency Care Provider		X	X	X	X		X
Researcher						X	

Patient or Legal Representative	x	x	x	x	x		

Table P-1 Sample Access Control Policies

This table shows that documents can be labeled with one or more of the codes on the columns, and results in the specified Functional Roles to be given access to that type of document. In this way, the XDS metadata informs the Role-Based Access Control (RBAC) decisions through self-describing sensitivity, known as confidentialityCode.

In the same way that the XDS metadata 'doctype' defines what the document is in terms of the clinical/administrative content, the confidentialtiyCode defines what the document is in terms of privacy/security content. For example although it might seem obvious that all ECG type documents are all likely to be the same from a privacy/security point of view, this is not mandatory and should not be presumed. A more specific example is that a medical summary document could easily contain observations that would fall into sensitive topics (in the USA - 42-CFR-Part-2); where as the vast majority of medical summary documents would not. Another example would be where a patient has requested that a specific report be handled more sensitively. Another example is an emergency data set that the patient wants made available to the widest possible audience. Only the publishing system knows this information. The confidentialityCodes should be looked at as a relatively static assessment of the document content privacy/security characteristics.

The confidentialityCode 'inside' the CDA does NOT need to correlate to the confidentialityCode found in the XDS Metadata. The main reason for this to be considered independent is that the confidentialityCode inside the CDA document is relative to the process/workflow that generated the document. If the original purpose for the document is to publish into a document sharing environment, then the codes are likely to be the same. When the document is re-purposed into a document sharing system, it will then be labeled with broader codes understood by the broader community. This re-purpose should NOT modify the original CDA document as that would be a modification.

Some have confused confidentialtiyCode with consents. These are totally different concepts. Access Controls are where all of the values including confidentialityCode, consents, user-role, permissions, and situation are brought together to make an Access Control decision. Consents likely have rules around documents with specific confidentialityCodes, but the binding of the rules to the codes is done in the Access Control step. The confidentialityCode is not the appropriate place to put dynamic rules. The confidentialityCode that is placed on a document at publication should be based on the document content, not based on current consents (there are exceptions, but they are very edge cases).

3.3 Building Upon Existing Security Environment

The IHE security and privacy model distributes the security and privacy duties to the edge systems like EHR, EMR, PHR, or other. The clinical applications in place today typically include the necessary basic security principles to protect patient data within the entity (e.g. hospital, clinic). These applications currently include controls to authenticate users, check that the users have rights to perform functionality (e.g. Role-Based-Access Control), and account for the actions of users within the application. These applications are installed within a facility and that facility has taken care to physically and electronically protect these applications with physical barriers, backup electricity, air-conditioning, backup of data, etc. For example, these are the types of controls currently required by the CCHIT certification criteria for Ambulatory EMR systems and In-Patient EHR systems in the USA (See http://www.cchit.org).

The emergence of Personal Health Records may introduce new policy requirements and controls both at the HIE level and at the local operational policy level. Individual participants should take this into account when evaluating their current risk profile. The Personal Health Record is an area that does not have regulatory controls in many countries (e.g. HIPAA in the USA has few regulatory controls on the Personal Health Record controlled by the patient).

The entities that are joining the HIE have experience in implementing the appropriate policies applicable within their entities and these have driven their choice of security mechanisms and influenced the appropriate implementation. These entities have some measure of control over their users (employees, contractors, patients). These entities understand their environment and have responsibility for implementing the controls for the locally appropriate authentication methods (passwords, smartcards, 2-factor token, etc). They can react quickly to provision, suspend, authorize, and de-provision users in a way that is sensitive to the employees' rights. As these entities join an HIE the clinical applications that touch the HIE can be seen as being applications within an entity that is participating in an exchange. The edge applications and its architecture need to incorporate the HIE policies and controls.

In healthcare, beyond the basic security principles, we must additionally be sensitive to patient care and safety. The applications closest to the patient are best informed for determining the context of the current situation. It is primarily at this level that emergency mode can be handled in a robust way (often called break-glass).

The IHE security and privacy model leverages the general security controls available in the edge applications in a complementary way to protect the assets of the HIE (it does not exclude to also exert some controls within the shared HIE infrastructure). The IHE security and privacy model is very careful to include security while allowing for flexible and safe provision of healthcare by individual participants. The IHE security and privacy model reinforces the need for these common basic security functionalities through the definition of the Audit Trail and Node Authentication (ATNA) profile. This same profile ensures that the edge systems are strongly authenticated to the HIE to ensure that only trusted systems are allowed to have access to the HIE.

For example, In Figure 3, we show how an Electronic Medical Record (or EMR) as an edge system is responsible for providing authentication of users, role-based access control, and audit logging. Because this system has proven that it accomplishes these functions it is given a digital certificate that allows it to communicate with the Document Registry and Document Repository. The EMR might extend its user-interface using a browser session, that is allowed access through the EMR, but this browser session is not allowed to talk directly to the Document Repository. Thus the end user may be using a browser, but this browser does not make a direct connection to the XDS document repository.

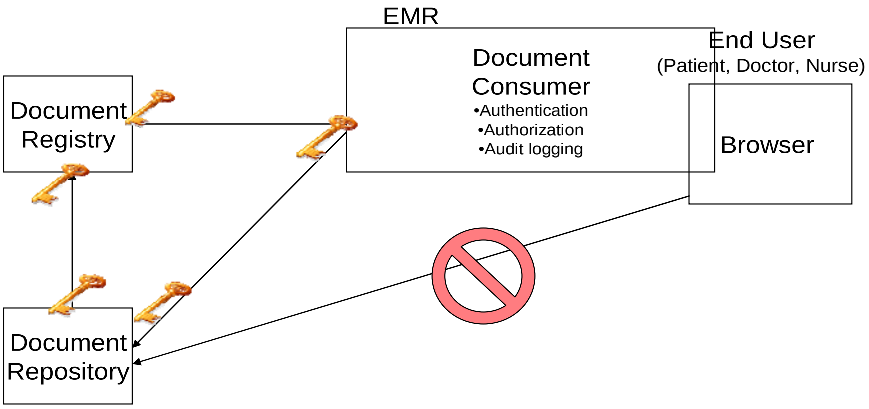

Figure 3: Distributed Security with system authentication and authorization

By authenticating all network communications, no un-authorized system will be allowed access to the HIE. The keys would only be distributed to systems that have proven that they have the right access controls and audit controls. The key management is not specified by IHE because there is a couple of good ways to manage the keys depending on the resources to be protected and flexibility necessary. For more information about how to manage these machine keys, please read the "Management of Machine Authentication Certificates" white paper by MITA at http://www.medicalimaging.org/policy/security.cfm.

Further details about the IHE profiles can be obtained by going to the IHE web site at http://www.ihe.net/Technical_Frameworks.

3.3.1 Centralizable Access Controls

Although the IHE Security and Privacy model pushes the access control decisions out to the edge systems, this is not the only way to implement access controls. The Document Registry and Document Repository know through strong network authentication which systems are making requests. They could use this system identity to deny access to specific information. The Cross-Enterprise User Assertion (XUA) Profile provides the user identity on the transactions so the Document Registry and Document Repository could enforce some level of Role-Based Access Control. The Document Registry additionally has direct access to the XDS Metadata including Patient identity to further enhance the access control decision. These same levels of access control could also be implemented using trusted web-services intermediaries that act upon the XDS transactions and either pass the request through or reject the request before it ever reaches the Document Registry.

In the previous sections we have discussed the topics of consent, confidentialityCode, user, functional role, and situation. Not all of these factors are known to the systems in the network including the XDS Document Registry. These are known gaps in the current standards. IHE is working with pilot projects around the globe and standards organizations to fill these gaps and look forward to expanding the IHE Security and Privacy model.

3.4 IHE Security and Privacy Toolkit

The IHE security and privacy profiles only define the interaction (network protocols) between logical applications and not the behavior within an application (e.g. user interface, clinical decision support, medications management). In many cases security and privacy controls can be implemented in application functionality. In other cases the principle needs to be handled in a general way in the HIE Policy. In both these cases, neither the functionality nor the policies are defined by the IHE profile.

This white paper does not describe in detail how the IHE profiles satisfy the principle but provides an overview of the profiles, their relevance and directs the reader to the individual IHE profile and topic within the profile. The following is a list of IHE profiles that can be leveraged to satisfy security and privacy requirements.

- Audit Trail and Node Authentication (ATNA)
- Consistent Time (CT)
- Basic Patient Privacy Consents (BPPC)
- Enterprise User Authentication (EUA)
- Cross-Enterprise User Assertion (XUA)
- Personnel White Pages (PWP)
- Digital Signatures (DSG)
- Notification of Document Availability (NAV)
- Cross-Enterprise Document Sharing (XDS)
- Cross-Enterprise Document sharing via Reliable messaging (XDR)
- Cross-Enterprise Document sharing on Media (XDM)

3.4.1 Basic Security

IHE recognizes that in healthcare, with patient lives at stake, audit control is the primary method of accountability enforcement. The profile that provides this basic security principle is Audit Trail and Node Authentication (ATNA). This profile makes three assumptions that leverage the edge system capabilities:

1. user authentication and Access Controls,
2. Security Audit Logs, and
3. Strong network authentication for all communications of sensitive patient data

These assumptions make up the first part of the ATNA profile. They require an assessment of the edge systems capabilities by an enforcement on the local entity of the HIE Policies around

Authentication and Access Controls. This part does not require any interoperability, but places functional requirements on the actors involved in the HIE.

> Note: Although beyond the scope of the HIE interoperability, it is worth noting that some IHE Profiles are applicable within the enterprise. The user authentication within the local entity could be accomplished using the Enterprise User Authentication (EUA) profile. The EUA profile leverages the Kerberos standard to allow for centralized authentication using a secure authentication service. The user attributes could be managed centrally using the Personnel White Pages (PWP) Profile, which leverages LDAP.

The second part of ATNA is Security Audit Logging. The profile includes a set of security relevant events and XML schema defining what to capture in an audit record when these security relevant events happen. The edge system is expected to support the recording of all of the security relevant events that might happen on the edge system. Once an event has happened in the HIE, it will be described in detail in an XML message and communicated to an Audit Record Repository.

The Audit Record Repository is expected to be able to do Filtering, Reporting, Alerting, Alarming, as well as forwarding of events to other HIE Audit Record Repositories. The more centralized this audit log analysis can be, the more easily it is to prove accountability across the whole HIE. The Audit Record Repositories can be centralized or distributed. The approach used by ATNA allows for one or more Audit Record Repositories in the HIE. Depending on the policies, each edge system may have their own Audit Record Repository, there may be a hierarchy, or there may be one for the whole HIE.

The following figure shows an Electronic Medical Record producing audit logs within the local Clinic. This local clinic’s audit record repository is configured to forward selected subset of messages that were triggered by activity with the HIE. This may be an automated process, manual reports filed on a regular basis, or only brought together when an incident invokes a log aggregation policy. During an HIE incident investigation there may be need to go back to the Clinic to do a detailed investigation. The HIE policy needs to cover this.

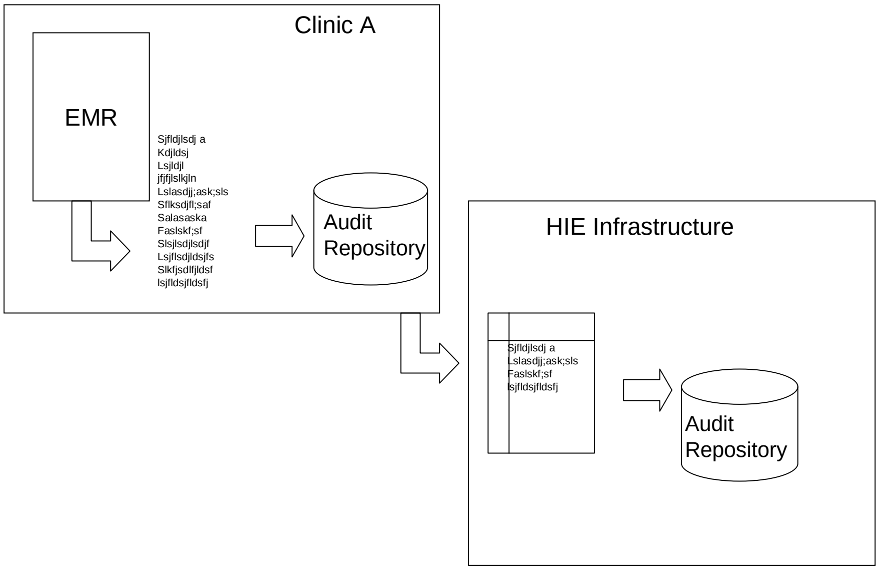

Figure 4: Audit Flow Down

Once it is known that the system will enforce Access Controls and Audit Controls then it can be connected via the HIE to other systems that have also been assessed positively. In this way these edge systems only talk to other edge systems that also agree to enforce the common HIE policies. This creates a basis for a chain of trust through accountability among all of the systems participating in the HIE. The communications between these trusted systems is also encrypted to ensure that only the trusted systems have access to the information collected in the audit trail.

4 IHE Security and Privacy Controls

The following is a breakdown of the security and privacy controls and in what way the IHE profiles can help. The following table shows the set of identified Controls (identified in section 2 above) as columns and the supportive IHE Profiles as rows. In this table a ‘D’ indicates a direct relationship. A direct relationship means that the Profile addresses the security and/or privacy principle. An ‘I” indicates an indirect relationship, meaning that the Profile assists with the principle. Further details on the ‘D’ direct relationships follow in this chapter. The indirect relationships are not further discussed.

Table 2: Profiles relationship to Controls

Security & Privacy Controls IHE Profile	Accountability	Identification and Authentication	Data Access	Confidentiality	Data Integrity	Non-Repudiation	Patient Privacy	Availability
Audit Trails and Node Authentication – ATNA	D	D	D	D	D	D	D	
Basic Patient Privacy Consents – BPPC				I			D	
Consistent Time – CT	D	I				D		
Enterprise User Authentication – EUA	I	D	I	I		I	I	
Cross-Enterprise User Assertion – XUA	I	D	I	I		I	I	
Document Digital Signature – DSG	D	D			D	D		
Cross-Enterprise Document Sharing XDS				D	D		I	D
Cross-Enterprise Document Reliable Messaging - XDR				D	D		I	D
Cross-Enterprise Document exchange on Media – XDM			I	D	D		I	D
Personnel White Pages – PWP	I	D	D			I		

4.1 Accountability Controls

ATNA: All systems must be assessed as trustable

ATNA: All systems only communicate with other trustable systems

ATNA: All systems must enforce access controls

ATNA: All systems detect the auditable events and produce audit messages according to the defined audit schema in the expected audit repositories.

CT: All systems are synchronized to the same time base thus audit logs are properly attested

DSG: records the identity of the signer of a document via a digital signature.

4.2 Identification and Authentication Controls

ATNA: All systems must have user authentication before allowing access to PHI

EUA: An enterprise user authentication system

PWP: A system for getting details on users (personnel)

XUA: Identify an authenticated principal in a cross-enterprise transaction

DSG: records the identity of the signer through the use of the private key. The presumption is that the user must have been authenticated prior to access to the private key.

4.3 Access Controls

ATNA: All systems must enforce access controls

PWP: A system for getting roles assigned to users

XUA: Inform the access control decisions

4.4 Confidentiality Controls

ATNA: communications encryption

ATNA: All systems must authenticate users before providing access to PHI

ATNA: Required audit log format and specific auditable events

XDS: All Queries are patient specific

XDS, XDM, XDR: Metadata has minimal PHI

- Integrity controls: Times, size, hash, oid, uri
- If Known: Author Institution, Author Name, Author Specialty
- HIE specific: Healthcare facility type, Practice Setting code, Patient Identifier number, Document Format Code
- Document MIME-TYPE
- Document Source Specific: Patient demographics (Full Name, Gender, Date of Birth, and Address)

XDR: A system for communicating documents directly between two systems reducing the threat to eavesdropping.

XDM: A system for communicating documents using media or over S/MIME

4.5 Data Integrity Controls

ATNA: Node Authentication with Certificates ensures non-trustable systems are kept out

ATNA: Integrity controls to ensure the transaction is whole

XDS: Integrity controls built into metadata to ensure the document lifespan is covered

XDS: Document management model ensures that documents are not removed but are deprecated with clear successors

XDS, XDM, XDR: Document model and standards formats ensure that the data can be maintained over long time

DSG: Certificate based Digital Signatures can be applied to the documents

XDS is document centric assuring Persistence, Stewardship, Potential for Authentication, and Wholeness.

ATNA: All actions are discoverable allowing for monitoring for appropriate use, test for leaks. Security is an actively managed process allowing for oversight and vigilance.

4.6 Non-Repudiation Controls

The Non-Repudiation Controls incorporate the Integrity Controls, but rely more specifically on the following controls:

DSG: Certificate based Digital Signatures can be applied to the documents

CT: All systems are synchronized to the same time base thus audit logs are properly attested

ATNA: All actions are discoverable allowing for monitoring for appropriate use, test for leaks. Security is an actively managed process allowing for oversight and vigilance.

4.7 Patient Privacy Controls

The XDS model at a high level supports a simple patient use consent policy allowing for the support of opt-in or opt-out depending on the way the specific HIE chooses. In this way a patient can choose to be included or not included in the HIE. This would be recorded at the edge application and controlled by that application.

In addition to this basic capability, the BPPC profile indicates the patient's willingness to participate in the HIE, or to NOT participate. The BPPC profile is sufficient enough to handle a small number of different policies that generally cover most types of patients' privacy consent.

The BPPC profile is not so extensive so as to handle individual patient's exceptions to the basic set of policies. IHE recognizes that there are patients that want to single out individuals that are authorized and individuals that must not be given access. This more advanced level of control is not readily expressible in current standards. There is ongoing standards work within HL7 and OASIS to address this.

A powerful feature of the IHE security and privacy model is a built-in accountability system. The ATNA profile's audit log can be examined for unacceptable behavior, and the HIE can react according to their Policy. For expressly sensitive documents for a specific patients, it might be best to either share these documents under a very restrictive policy, or keep such sensitive data within the edge application EMR and not share any of that sensitive patient's data with the HIE.

4.8 Availability Controls

Availability Controls are more environmental in nature, that is they are provided by the infrastructure that is used to build the HIE. There are some key aspects of the IHE profiles that are still highly important to maintaining availability:

XDS: Document model and standards formats (IHE Content Profiles from Clinical Domains such as Patient Care Coordination, Radiology, Laboratory, etc.) ensure that the data can be maintained over long time.

XDS is all standards-based ensuring that the information managed in XDS is not locked into a proprietary system.

5 Conclusion

This paper has shown that there is a good foundation of security and privacy controls built into the IHE family of Profiles applicable to HIE solutions. The IHE IT Infrastructure Planning Committee is looking for feedback on this White Paper, issues that the readers would like to see added, and any suggestion for improvements. Comments should be sent to:

IT Infrastructure Planning Committee Secretariat
Healthcare Information and Management Systems Society (HIMSS)
ihe@himss.org

5.1 Future efforts

One of the gaps is in the handling of complex individual consents. These issues are currently being worked on in standards organizations with the expectation that more complex privacy consents can be handled in the future. For now these complex privacy consent conditions can be handled through selective publication.

There is room for optimizations to the solution that are underway in the standards organizations. Centralized and/or Federated access control decisions using XACML, services that can determine if a care provider has a legitimate treatment relationship with the patient, and further refinement of authentication assurance levels. These improvements and optimizations are expected but require a maturity in many of the newer standards and technologies that are necessary to handle such sensitive data and such critical patient safety. Their deployment can easily be considered as future evolutionary step for HIEs that have chosen to rely on the current portfolio of IHE Profiles. There are new use-cases currently focused in the Quality Domain around data mining activity, and aggregate data access. As these use-cases are developed, IHE will look at the security and privacy implications. This might possibly include de-identification through pseudonymization, blanking and anonymyzation.

5.2 Building Today

The IHE profiles provide the basic infrastructure necessary to build a secure HIE. The HIE must also have good governance guided by Policies. These HIE Policies should include a recurring risk assessment. The HIE must continue to check for consistency in recommended standards such as those profiled by IHE. Given that important information needs to be appropriately secured and managed by edge applications in a way consistent with the HIE, participants should leverage the edge applications security and privacy capabilities and configure them to enforce the HIE policies. This type of a bottom-up secure HIE system is available today and has been shown in Connectathon implementation demonstrations as well as used in multiple pilot projects in the USA and Europe.