

**ACC, HIMSS and RSNA
Integrating the Healthcare Enterprise**

5



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

10

**Draft for Public Comment Version
Comments due August 15, 2007**

15

Contents

Contents 1

1 Introduction..... 2

2 Scoping Security and Privacy..... 4

20 2.1 International Data Protection Principles..... 4

2.2 Policies and Risk Management 4

2.3 Technical Security and Privacy controls 7

3 Applying Security and Privacy to an HIE 9

3.1 Building Upon Existing Security Environment..... 9

25 3.2 IHE Security and Privacy Toolkit 10

3.3 IHE Security and Privacy Controls 12

4 Conclusion 16

4.1 Future efforts 16

4.2 Building Today 16

30

1 Introduction

35 Regions 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 IHE has proposed that a basic method of providing a HIE is through an infrastructure that allows for the sharing of clinical documents about a patient in a way that allows for long term use. This infrastructure is made up of a 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.

40 The organizers of the HIE need to implement basic security principals in order to offer a security model to protect the HIE information exchanges. The architecture put forth by IHE is to share discrete information in the form of documents. These 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
45 expectation that in the future they can be used to provide better healthcare treatment to that same individual patient.

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
50 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.

55

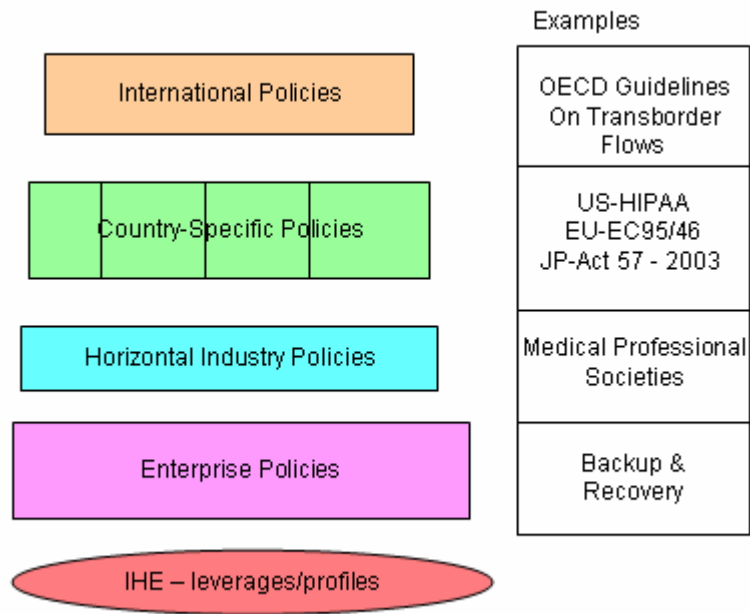


Figure 1: Policy Environment

60 The Policy Environment is made up of many layers of policies. These policies work together in a
65 hierarchic way to interlock. We will introduce some of these different 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.

2 Scoping Security and Privacy

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

2.1 International Data Protection Principles

- 70 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.
- 75

In the context of this paper, these data protection principles will be scoped to the IHE relevant policies and understood in the context of the IHE risk environment. The technical controls that are relevant to IHE are distilled below.

80 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.

- 85 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 Framework, Volume 1: Appendix “L” 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 implementers. It is therefore the duty of system implementers to take this guidance into account as part of their Risk Management practices
- 90

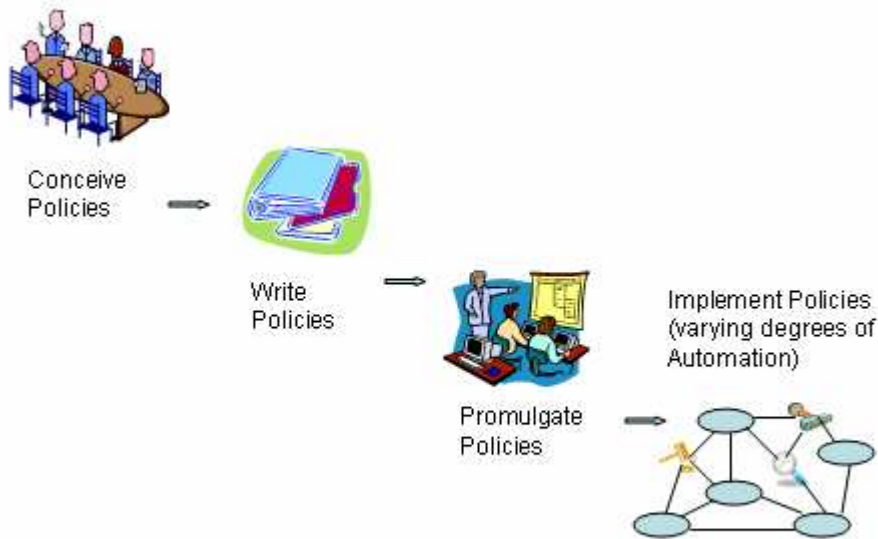


Figure 2: Policy Lifecycle

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

For example implementers need to be aware of different kinds of policies that need to be harmonized with local enterprise policies:

- 100 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 in 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
105 policies
f) Policies on training and awareness
g) Policies on user provisioning and de-provisioning within affinities (and local operations policy)
h) Policies on emergency mode operations
110 i) Policies on acceptable network use and protections
j) Policies on 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

- 115 n) Policies on the availability of the HIE (is the HIE considered life critical, normal, or low
priority)
o) Policies for maintenance
p) Policies for length of time that information will be maintained in the HIE
q) Etc

120

These policies are not a flat set, but often can be seen as a cascade. A good example of this is the cascade of policies related to access to a patient's data. At the Community level 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 them-selves in their own privacy consent where specifically a hostile neighbor might be named.

125

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.

130

- 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.

135

140

Often times the emergency room is considered as an emergency mode, but the emergency room 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.

145

Policy development is frustrated by apparent conflicts in policies. These conflicts are often superficial 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 superficial policy conflict is in records retention requirements at the national level vs at the medical level. Retention of records is fixed at a short

150

period after death, yet if the patient has black lung then the records must be preserved well beyond.

155 **2.3 Technical Security and Privacy controls**

Based on the experience of the IHE participants through experience 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 expectation of general Policies and Security Risk Management.

These security and privacy controls can be used to enforce the:

- 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.
- 165 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.
- 170 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.
- 175 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 a prescription.
- 180 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.

185 For example: Two of the OECD data protection principals are 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.
 - 190 • Access Controls.
 - Confidentiality Controls.

- Patient Privacy Controls.
- I want to be sure the data are not modify by some one who doesn't have the right for that
 - Identification and Authentication Controls.
 - 195 • Access Controls.
 - Data Integrity Controls.
- I want to be sure the data can be retrieve when needed
 - Availability Controls

Accountability:

- 200 • I want to be sure who is doing action
 - Identification and Authentication Controls.
- I want to know what is done by who
 - Accountability Controls.
- I want to be sure what has been done cannot be denied
- 205 • 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 given the IHE profiles.

3 Applying Security and Privacy to an HIE

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

This section will show how the existing security controls in standalone system are leveraged and extended when connecting them into an HIE.

3.1 Building Upon Existing Security Environment

215 The IHE model for participants presumes that clinical applications in place today 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, to check that the users have rights to perform functionality (e.g. Role-Based-Access Control), and to account for the actions of users within the application. These applications are installed within a facility and that facility
220 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>).

225 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 and 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 has few regulatory controls on the Personal Health Record controlled by the patient).

230 The entities that are joining the HIE have experience in implementing the appropriate policies for their entities and these have driven their choice of security mechanisms and influenced the appropriate implementation. These entities have some measure of control (there will be variations in the entities) 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
235 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 at the edge of the entity that are participating in an exchange. As such the edge applications and their architecture need a common set of policies and controls to apply to the edge application, or edge system.

240 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 only at this level that emergency mode can be handled in an expedient way (often called break-glass).

245 The IHE model leverages the general security controls available in the edge applications in a complementary way to protect the assets of the HIE. The IHE model is very careful to include

250 security while allowing for flexible and safe provision of healthcare by individual participants. The IHE 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.

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

3.2 IHE Security and Privacy Toolkit

255 When implementing an HIE we begin by recognizing that in the current IHE security model the ‘edge application’ we must meet the necessary general security controls shown above. The IHE models only define the interaction (network protocols) between logical applications and not the behavior within an application (e.g. clinical decision support, medications management). In many cases the choice of implementation for security is application functionality which provides the control for security and privacy. 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.

260 This white paper will not fully describe how the IHE profiles satisfy the principle but provide an overview of the profiles and pointers to direct 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)
- 270 • Cross-Enterprise User Assertion (XUA)
- Personnel White Pages (PWP)
- Digital Signatures (DSG)
- Notification of Document Availability (NAV)
- Cross-Enterprise Document Sharing (XDS)
- 275 • Cross-Enterprise Document sharing via Reliable messaging (XDR)
- Cross-Enterprise Document sharing on Media (XDM)

3.2.1 Basic Security

280 IHE assumes that audit control is the primary control method of accountability enforcement. The profile that provides the basic security principle is the Audit Trail and Node Authentication (ATNA) profile. This profile has three components that leverage the edge system capabilities.

The first part of the ATNA profile is an assessment of the edge systems capabilities to enforce the HIE Policies around Authentication and Access Controls.

285 The second part of ATNA is Security Audit Logging. The profile includes a set of security relevant events and a schema for defining what to capture in the audit 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 system. Once an event has happened in the HIE, it will be described in detail in an XML schema and communicated to an Audit Record Repository.

290 The Audit Record Repository is expected to be able to do Filtering, Reporting, Alerting, Alarming, as well as forwarding of events to other HIE system 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 system 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.

300 The following figure shows an EMR producing audit logs to the local Clinic, with a subset of these audit logs being forwarded to the HIE Infrastructure. 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.

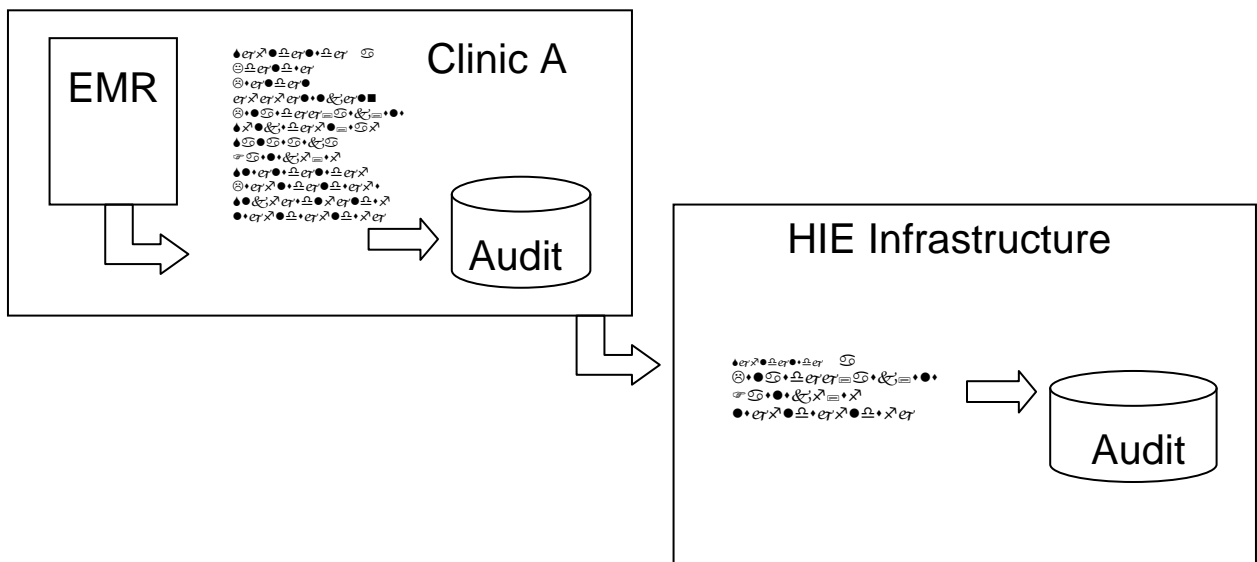


Figure 3: Audit flowdown

305 Once it is known that the system will enforce Access Controls and Audit Controls then it can be connected to other systems that have also been assessed positively. In this way these edge systems only talk to other systems that also agree to enforce the common policies. This creates a

DSG: records the identity of the signer

3.3.2 Identification and Authentication Controls

325 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 a principal in a cross-enterprise transaction

330 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.

3.3.3 Access Controls

ATNA: All systems must enforce access controls

PWP: A system for getting roles assigned to users

3.3.4 Confidentiality Controls

335 ATNA: Encryption with 3DES or AES

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

- 340
- 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
- 345
- Document Source Specific: Patient demographics (Full Name, Gender, Date of Birth, and Address)

XDR: A system for communicating documents directly between two systems

XDM: A system for communicating documents using media

3.3.5 Data Integrity Controls

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

ATNA: Integrity using SHA1 to ensure the transaction is whole

XDS: Integrity (SHA1) 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

355 XDS: 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 family is all standards based ensuring that the information managed in XDS is not locked into a proprietary system

360 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.

3.3.6 Non-Repudiation Controls

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

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

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.

370 3.3.7 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.

375 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 powerful enough to handle a small number of different policies that generally will cover most types of patients' privacy consent.

380 The BPPC profile is not powerful enough to handle individual patient's exceptions to the basic set of policies. We recognize 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.

385 A powerful feature of the IHE 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 patients, it might be best to keep their data within the edge application EMR and not share any of that patient's data with the HIE.

3.3.8 Availability Controls

390 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 ensure that the data can be maintained over long
time

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

4 Conclusion

400 This paper has shown that there is a good foundation of security and privacy controls built into the IHE solution. There are additional standards and profiling work necessary. The purpose of this white paper is to inform the public of the current solutions and to invite comment on the future efforts.

4.1 Future efforts

405 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, for example centralized access control decisions and legitimate relationship with the patient. These improvements and optimizations are eagerly 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.

410 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 anonymization.

4.2 Building Today

415 The IHE profiles provide the basic infrastructure necessary to build a secure HIE. The HIE must also have good governance guided by Policies to contain the IHE principles. 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,
420 participants should leverage the edge applications security and privacy capabilities and configure them to enforce the HIE policies.

This type of a bottoms-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.

425