Clinical Record Use Cases

Title:	Clinical Record Use Cases
Terse Description:	Control of the creation, maintenance, and access of medical records and messages coded in XML.
Version:	v0.1
Submitted by:	Fred Moses
Date:	September 4, 2001

Summary

Access to medical records is governed by ethical and legal privacy requirements and the preferences of the patient. This use case and its variants illustrate related confidentiality needs.

Scope

Medical record creation, storage, access, and messaging system and its users.

Actors

1. Creators and readers of medical documents such as physicians and other health care givers
2. Patients
3. Those associated with Patients who have access privileges
4. Payers
5. Institutions (HMOs, government bodies) permitted access.

Assumptions

The Health Level Seven Clinical Document Architecture and usage drawn from discussions about it form reasonable models for the creation, management, and accessing of medical information about individual patients. The interpretation of the HL7 standards is strictly that of this writer.

Non-technical Factors

HIPAA and other privacy legislation, medical ethics.

Process Sequence

Flow diagrams are not provided in this version.

Primary Process Flow

A physician creates a record with administrative, medical, and privacy content, signs it, and has it stored (in XML format) in a records system.

Key Points:

- Other personnel may collect portions of the record, such as the administrative information.
- Access policy must have granularity at the level of elements within the document and individuals within the actor population.
- Access policy must be included with the document.
- The document must have a nonreputable signature.
- Once signed, the document itself may not be modified.

Alpha Process Variant: Record retrieval

A physician or other permitted actor retrieves all or parts of a record for review or transmission to other parties.

Key Points:

- The portion of a document that may be retrieved depends upon the requestor and privacy conditions included in document. For example:
  - Patient restricts access to specific administrative info (address and phone number) to prevent abusive ex-spouse from finding her.
  - Restrictions extend beyond the originating organization and follow the record or message to another. (This may warrant the encryption of restricted portions.)
  - Differential access restrictions for especially private information such as psych notes. That is, while most of a record may be made available to a new actor, restrictions may be applied in the process.

Beta Process Variant: Record transmittal

A permitted actor retrieves all or part of a record for transmission to other parties. They must be bound by the same restrictions that already apply to the information.

Key Points:

- Restrictions extend beyond the originating organization. Encryption may be a means of enforcing this.
- Necessary agreements between originator and receiver are beyond the scope of this use case.

Gamma Process Variant: Record addendum

A physician or other caregiver creates an addendum to a record with administrative, medical, and/or privacy content, signs it, and has it stored (in XML format) with the existing record in the records system.

Key Points:

- Since signed records or portions of them may not be modified, some form of a attachment or addendum must be used.
- Changes in access permissions may affect the previously existing document and any addenda. Both patient and care giver can add restrictions. Only the patient can cause restrictions to be removed. (See the cases regarding information withheld from the patient, below.)
- Any addenda to the access policy must be included with the document.
- Should a form of version control be applied?
- The result must have a nonreputable signature.
- Once signed, the addendum itself may not be modified.

Delta Process Variant: "Breaking the glass"

A patient arrives at the emergency room unconscious. Caregiver(s) need to be able to assume special privileges in order to gain access to information that was restricted, but may be critical in the patient's care.

Key Points:

- There need to be people, possibly outside the normal flow, who have special privileges.
  - Do they need to possess a special decryption key?
  - Do there need to be multiple decryption keys such that no single person can break glass.
- When extraordinary measures are invoked, should a standard mechanism attach a note to the record? See the comment regarding version control, above.

Epsilon Process Variant: Information is withheld from patient

A psychiatrist receives information that s/he believes could be harmful to the patient or others if disclosed to the patient. In accordance with the law in the patient's state, the psychiatrist marks this information as not

to be disclosed to patient. The patient requests access to his/her psychiatric records. Access to the restricted documents is denied.

Key Points:

- The patient isn't the legal owner of his/her records. Except in legally identified cases such as this, however, the patient has the right to see his/her own record. Thus, there is a policy that circumstances may modify.

Zeta Process Variant: Patient overrides restrictions

The patient in the previous example obtains an override of the restrictions through legal recourse. Access is permitted.

Key Points:

- Legal maneuvers are outside the scope of this use case.
- There is a need for attaching new access privileges to an existing document.

Glossary

Caregiver

Physician, nurse, or other person providing health care. The HIPAA rules gives strict definitions for this and other personages and devices associated with the health care process. These are outside the scope of this use case. An informal meaning will suffice.

HIPAA

Health Insurance Portability and Accountability Act of 1996 - An act of Congress specifying, among other things, privacy standards for medical records. This is augmented by Department of Health and Human Services rules. See the Web site given below.

Nonreputable signature

A signature signed in such a fashion that the signer couldn't refute it. See, for example, the XMLD specification for which there is a link below.

References

Health Level Seven - http://www.hl7.org/

- Structured Documents Technical Committee
- XML Special Interest Group
- Modeling and Methodology

HIPAA - http://www.hcfa.gov/hipaa/hipaahm.htm

XML - Signature Syntax and Processing - http://www.w3.org/TR/xmldsig-core/

ebXMLRegistry-Restricting Read-Write Access

Title:	ebXMLRegistry-Restricting Read-Write Access
Terse Description:	**Limiting read-write (read, approve, deprecate, remove) access for the Registry contents to specified subjects.**
Version:	V 0.5
Submitted By:	Suresh Damodaran
Date:	Sept 4, 2001

Summary

Scope

Actors:

1. Registered User: Affiliated with either the Submitting Organization or Partner Organization.
2. Registry Guest: Is not affiliated with either the Submitting Organization or Partner Organizations.
3. Submitting Organization: Who submits RegistryObject
4. Partner Organization: Partners of submitting organization

Assumptions

It is assumed that the information on Registered Users affiliated with a Partner or Submitting Organization is available in the Registry. Registered User and Registry Guest are authenticated.

Non-Technical Factors

Process Sequence

Primary Process

A Submitting Organization (SO) submits a RegistryObject to a Registry. SO also submits to Registry an AccessControlPolicy associated with the RegistryObject. This AccessControlPolicy allows only selected Users of SO or Partner Organizations to have read, approve, deprecate, and remove access of the RegistryObject. All objects in the registry have a unique id specified by *Universally Unique Identifier (UUID)* and must conform to the format of a URN that specifies a DCE 128 bit UUID as specified in UUID [ebRS:Section 7.3.1, UUID].The Registered Users affiliated with Partner Organizations or Submitting Organization may be specified in the AccessControlPolicy using Identity, Role, or Group information.

Flow Diagram

Flow Key Points

Alpha Process Variant

Flow Diagram

Key Points

Beta Process Variant

Flow Diagram

Key Points

Glossary

References

[ebRS] ebXML Registry Services Specification

- http://www.ebxml.org/specs/ebRS.pdf

[ebRIM] ebXML Registry Information Model 1.0

- http://www.ebxml.org/specs/ebRIM.pdf

[UUID] DCE 128 bit Universal Unique Identifier

- http://www.opengroup.org/onlinepubs/009629399/apdxa.htm#tagcjh_20
- http://www.opengroup.org/publications/catalog/c706.htm
- http://www.w3.org/TR/REC-xml

Online Access Control

Title: Online Access Control
Terse Description: Policy determines if access should be allowed to online resources
Version: 1.0
Submitted By: Hal Lockhart
Date: September 4, 2001

Summary

A user or process in an online environment makes a request of an online server. A policy is evaluated to determine if the access should be allowed. Elements within the server act as a Policy Enforcement Point, either allowing or denying access.

Scope

The scope includes any online server application environment, such as HTTP; Java Applications, including Servlet, Java Server Pages and J2EE; and CORBA. It could also apply to other Internet protocols, such as ftp or pop3. It could apply to legacy environments, such as mainframe transaction processing. It could also apply to emerging environments, such as XML Protocol. The access control is typically non-discretionary, but many of the existing schemes are based on discretionary methods, e.g. ACLs.

Actors

1. System Entity that originates the request,
2. Server (PEP),
3. PDP

Assumptions

Non-technical Factors

Many of these environments have existing access control schemes associated with them. However the existence of a number of third party Access Management products with capabilities not present in the existing schemes suggests that they do not completely meet user requirements. Furthermore, since distributed applications are often built with a combination of these technologies, the use of multiple schemes is both inconvenient and error prone.

Process Sequence

Primary Process Flow

1. System Entity makes application request to Server containing PEP
2. PEP requests policy decision from PDP specifying target (local or remote)
3. PDP locates all applicable policies
4. PDP obtains necessary policy inputs from PIP (local or remote)
5. PDP evaluates policy to determine if access should be allowed
6. PDP informs PEP of decision
7. PEP permits action or returns error
8. [Optional] PDP makes determination to record information in Audit trail base on same or different inputs

Targets
The target of a request depends on the environment. In a Web environment it is an HTTP or HTTPS URL or the path component of the URL. This may be qualified by the HTTP operation specified, however this may be omitted because it is not possible in general to determine what the semantic of the particular request may be, e.g. Read or Write. In a remote invocation environment, the request typically specifies a method on an object. However, EJB security makes it possible to distinguish among different signatures on the same method. There is also utility to providing for targets that are arbitrary strings that may be meaningful to an application.

Conditions
The decision to allow access may be based on any or all of the following criteria.
- User possess a specified attribute (member of organization)
- User possesses a specified attribute with a specified value (member of Admin group)
- User possesses a specified numeric attribute that matches a numeric test against a constant (transaction limit > 1000)
- Current time is in specified range (between 9AM and 5PM)
- Current day of week is as specified (Saturday or Sunday)
- Client IP Address or DNS name is as specified
- Server IP Address or DNS name is as specified
- User authenticated using specified method (PKI)
- Connection is protected (TLS in use)

It should be possible to combine these conditions using the standard Boolean operators.
The normal consequence of policy evaluation is to allow or deny access. A policy decision may also be made to generate an Audit Trail record corresponding to the request. In this case, all the above criteria may be used and in addition:
- Was the request allowed or refused

Audit could be a provisional result of the decision, however this is inconvenient for two reasons:
- The final criterion mentioned applies to the audit decision and not to the authorization decision.
- It is frequently desired to enforce access control and not audit or generate audit records without checking access.

For both of these reasons it is simpler to have distinct Authorization and Audit Trail policies, instead of treating them as multiple consequences to a single policy.

Flow Diagram

Key Points
- A wide variety of resources can the target of the policy.
- Policy inputs include many other factors than subject attributes. In fact subject attributes may not be used at all in some decisions.
- The protocol used to make the request is irrelevant to the policy decision, except for its security properties

Alpha Process Variant

It is also possible to support lazy Authentication. This is an explicit part of the HTTP and Servlet protocols. In step 4, if the PDP determines that authenticated subject attributes are a required policy input and the user has not previously authenticated, he or she may be challenged to authenticate at that time.

Flow Diagram

Key Points
- Lazy Authentication

Beta Process Variant

Another variant occurs when the PDP recognizes that the policy evaluation failed because some factor that the requestor may be able to alter. Examples include:

- An insufficiently strong authentication method was used, or
- The communications channel is inadequately protected.

By signaling the problem to the application or the user, it may be possible to remedy the deficiency. Even when user action is not required, it may be desirable for performance reasons to only gather certain inputs once it is known they are needed. For example, a reverse DNS lookup of the client's IP address may be omitted unless specifically required.

Flow Diagram

Key Points

- Detailed feedback of reasons for failed policy evaluation

Glossary

References

Policy Provisioning

Title: Policy Provisioning
Terse Description: Policies are distributed from PRPs to PDPs
Version: 1.0
Submitted By: Hal Lockhart
Date: September 4, 2001

Summary

Previously created or modified policies are transferred from a Policy Retrieval Point (PRP) to a Policy Decision Point.

Scope

The scope includes any environments where PDPs utilize policies made available from a PRP.

Actors

1. PRP
2. PDP

Assumptions

Non-technical Factors

Process Sequence

Primary Process Flow

1. In this use case, the PDP simply requests policies from the PRP. The PDP might initiate the request based on elapsed time since the last update or some other criterion.

Flow Diagram

Key Points
- A reliable protocol to upload policies.
- The type of policy representation is irrelevant.

Alpha Process Variant

In this case, the PRP notifies the PDP that new policies are available. The PDP can then request the policies as in the previous case.
There are two reasons for this scenario as compared to having the PRP push policies to the PDP.
1. The PDP may be resource constrained. This allows it to control when and how it updates its policies.
2. The second part of the protocol is exactly the same as the Simple Pull, thus simplifying specification, implementation and testing.

Flow Diagram

Key Points
- PDP is notified when policies have changed.
- PDP controls the transfer process.

Glossary

References

SAML Authorization Decision Request and Assertion

Title: SAML Authorization Decision Request and Assertion
Terse Description: Policy inputs are conveyed between a PEP and PDP or between a PDP and a PIP
Version: 1.0
Submitted By: Hal Lockhart
Date: September 4, 2001

Summary

A PEP formulates a SAML request for an Authorization Decision, by specifying the policy inputs that apply. A PDP replies with an assertion that also specifies the policy inputs applied to the decision. The PDP may also request the necessary input values from a PIP, which in turn returns the values.

Scope

The scope includes any environments where SAML Authorization Decision Requests and Assertions are used or where a PIP is located remotely from a PDP.

Actors

1. PEP
2. PDP
3. PIP

Assumptions

Non-technical Factors

Process Sequence

Primary Process Flow

1. A PEP requests a SAML Authorization Decision Assertion, specifying the policy inputs.
2. The PDP determines that it lacks some of the inputs required for policy evaluation. It requests additional data from the PIP.
3. The PIP replies with the necessary inputs.
4. The PDP evaluates the relevant policies and issues the Authorization Decision Assertion, specifying the policy inputs utilized.

   Flow Diagram

   Key Points
   - A syntax to identify policy inputs and specify their values.

Glossary

References