Patient Data Privacy for eHealth Services

The Attribute Based Access Control (ABAC) solution

The Center for eHealth in Sweden coordinates the efforts of county councils and regions in the establishment of national eHealth services.

Security Infrastructure

Within this framework, the national healthcare security infrastructure BIF is maintained. The overall objective is to provide a secure infrastructure to meet patient privacy requirements while granting authorized care providers access to the information they need. BIF controls authentication and authorization for eHealth services and provides audit logging and other security functions. It ensures care providers comply with the Patient Data Act from 2008 and privacy mandates of the general Personal Data Act. The aim is that all care providers, whether public or private, will use these services for exchange of patient data. In total, BIF includes nine infrastructure components:

1. Services for strong authentication using smart cards and a PIN code
2. Services for authorization using XACML[1] combined with a national directory for attributes
3. A patient consent service where patient consent or blocking preferences are registered for nation-wide use
4. A “care relation” service used to establish whether a valid care relation exists between a care provider and a given patient
5. Audit logging services which record security related events
6. Log analysis tools used to monitor events and to detect possible intrusions etc.
7. EHR disclosure service dependent on patient detriment assessments.
8. Event-related notification services
9. Context controls used to verify that information displayed on-screen always relates to the correct patient ID.

[1]**XACML** stands for “eXtensible Access Control Markup Language”. The standard defines a declarative fine-grained, attribute-based access control policy language, an architecture, and a processing model describing how to evaluate access requests according to the rules defined in policies.

Standards Based Authorization

The XACML-based authorization engine gets information about users from trusted directories with information about care providing entities, their staff members' roles and competencies etc. It combines this with data from services about care-relation and patient consent registrations as well as data describing the accessed records and the context in which access is requested.

The XACML Policy Decision Point then determines whether an access request complies with applicable regulations or not.

The policy framework handles different types of use cases in which existing care relations, patient consent and/or information blocking preferences may impact authorizations differently:

1. Requests within a care providing unit
2. Requests from other units belonging to the same care providing entity
3. Requests made via the national patient summary service from units in other care providing entities.

Requests made from outside the care providing unit require an active choice. By default, authorized users are restricted to the current unit's "own" information. Other unblocked information can be accessed on demand only. Users are then prompted to confirm that they have a valid purpose of use.

The richness of the XACML policy language helps capture the many context-related aspects needed for an access control decision.

- XACML combining algorithms are used to create a hierarchy of overruling principles where conflicting rules may be applicable ("yes, in this context, being the patient's doctor, you have a valid purpose of use, but no, your patient has registered a blocking preference on parts of the information you want to access, but then again, if this is an emergency…").
- XACML obligations efficiently handle use cases involving an active choice and "break the glass" scenarios in emergencies when a patient is unable to make a consent declaration.

The patient summary service was tested during 2008 and 2009. It has been used in production since September 2009 and a new version was planned for 2015.

> **The XACML solution is provided by Axiomatics, which is the world leader in this field.**
>
> *- Mats Hagner, Product Lead Manager, Swedish Healthcare Advisory Organization*

Find out how you can secure your information assets without hindering your business. Contact **webinfo@axiomatics.com** today to learn more about our dynamic authorization solutions.

AXIOMATICS

Axiomatics, the leading provider of fine-grained and attribute-based access control (ABAC), has delivered the authorization engine for the world's largest XACML-driven eHealth initiative, the nation-wide eHealth services in Sweden.

525 W Monroe St., Suite 2310
Chicago, IL 60661, USA
Tel: +1 (312) 374-3443

Västmannagatan 4
S-111 24 Stockholm, Sweden
Tel: +46 (0)8 51 510 240