Foundation for Research and Technology - Hellas, Institute of Computer Science

Information Systems Laboratory

HACEF (Health Access Control Enforcement Framework)

Overview

HACEF is a **privacy-aware access control framework** that provides secure access to sensitive patient data as specified in a Patient Health Record (PHR). A PHR is a collection of various types of data related to a patient and is provided by healthcare professionals (medical doctors from public hospitals or private practice), clinics or hospitals (clinical observations or readings from various monitoring devices) and the patient himself/herself. The data in a PHR may be of administrative nature (e.g., the patient’s sex or age), or of medical nature (e.g., known allergies, illnesses, treatments). HACEF provides access control over data that are static (e.g., administrative data), dynamic (e.g., age, known allergies) and streaming (e.g., periodic measurements of vital signs in an intensive care environment).

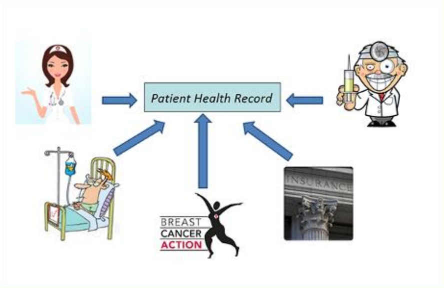
Access to a PHR is governed by the EU Data Protection Directive, which requires the **patient’s informed consent** for third parties to access his PHR. In more detail, the patient should authorize access to his data, specifying explicitly who can access which parts of his PHR, when, and for which purpose.

HACEF uses **access control enforcement techniques** to ensure the selective exposure of the information contained in a PHR according to the patient’s consent. To do so, an abstract model is employed, which records the access labels of explicit or implied information objects. In this model, an object's access label is an expression that depends only on the data and not on the access privileges as specified by a patient (that may differ between applications and even for the same application between accessing entities).

The **benefits** of using such a model are multiple. First of all, the abstract expressions for the implied information objects are computed only once. Moreover, the same expression may be associated to various different access control policies and such policies allow determining the possibility to access the information object at query time. Thus, any changes that may affect access to an object (e.g., editing a policy, experimenting with new access policies, the use of a new application on the same data, changes in the data and/or its accessibility) require no recomputation and automatically apply in future queries.

Target Domains

HACEF is currently targeted towards the medical domain. However, the abstract access control model on which HACEF is based can be used in all domains where there is the need to control the access to sensitive information; this includes financial, government, transport and communication data, among others. The main benefits of HACEF appear in domains where the same data can be accessed by different applications, changes are frequently applied on the data and the access policies are dynamic.

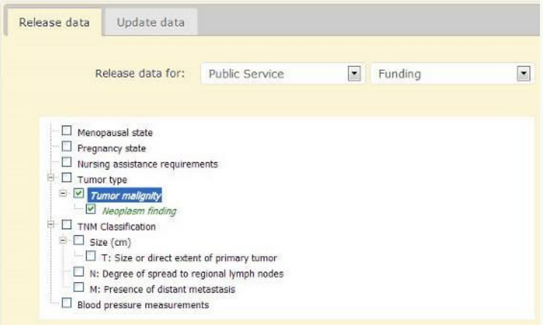


Description

HACEF uses **open source technologies** such as the MonetDB open source columnar database management system to store sensitive data, accessing entities and access privileges.

To prove the applicability of our approach, we have developed a custom-made Personal Health Record Application (PHRA). PHRA is a web application using JSP technology on top of the HACEF platform. The patient can login to PHRA using his credentials, and then select which accessing entities can access which parts of his/her PHR and for which purpose; this amounts to filling in a consent form and determine the access privileges that various accessing entities have on the patient's medical information. A regular user can define new or modify existing consent forms.

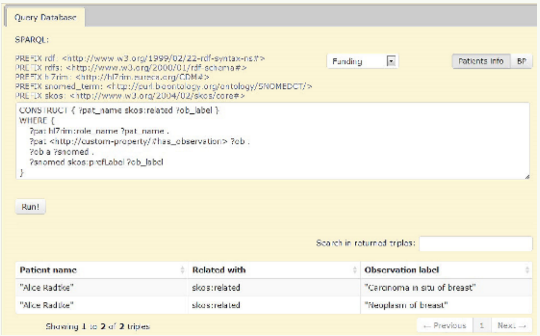
An accessing entity (for instance, a doctor) can login to the system by providing his/her credentials, and query the data; the results of his/her query will be appropriately filtered depending on his/her access privileges, as specified by the patients' consent forms.



Release data for: Public Service Funding

- □ Menopausal state
- □ Pregnancy state
- □ Nursing assistance requirements
- □ Tumor type
  - ☑ *Tumor malignity*
    - ☑ *Neoplasm finding*
- □ TNM Classification
  - □ Size (cm)
    - □ T: Size or direct extent of primary tumor
  - □ N: Degree of spread to regional lymph nodes
  - □ M: Presence of distant metastasis
- □ Blood pressure measurements

Release Form



SPARQL:

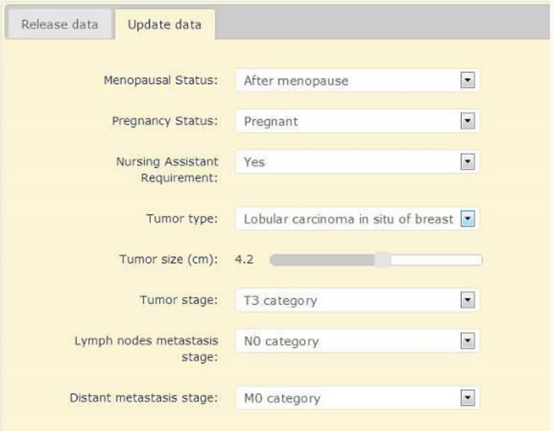
```
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX hl7rim: <http://hl7rim.eureca.org/CDM#>
PREFIX snomed_term: <http://purl.bioontology.org/ontology/SNOMEDCT/>
PREFIX skos: <http://www.w3.org/2004/02/skos/core#>
CONSTRUCT { ?pat_name skos:related ?ob_label }
WHERE {
   ?pat hl7rim:role_name ?pat_name .
   ?pat <http://custom-property/#has_observation> ?ob .
   ?ob a ?snomed .
   ?snomed skos:prefLabel ?ob_label
}
```

Search in returned triples:

Patient name	Related with	Observation label
"Alice Radtke"	skos:related	"Carcinoma in situ of breast"
"Alice Radtke"	skos:related	"Neoplasm of breast"

Showing 1 to 2 of 2 triples

Querying Patient Data



Menopausal Status:	After menopause
Pregnancy Status:	Pregnant
Nursing Assistant Requirement:	Yes
Tumor type:	Lobular carcinoma in situ of breast
Tumor size (cm):	4.2
Tumor stage:	T3 category
Lymph nodes metastasis stage:	N0 category
Distant metastasis stage:	M0 category

Updating Patient Consent Form

Additional Information

A video demonstrating a specific usage scenario employing HACEF can be found at:

https://www.youtube.com/watch?v=-wYbiWvTfyE

HACEF demo video

Contact details: **Irini Fundulaki**

fundul@ics.forth.gr

www.ics.forth.gr/isl