Assuring Privacy of Medical Records in an Open Collaborative Environment

A Case Study of Walloon region's eHealth Platform

Syed Naqvi , Gautier Dallons, Arnaud Michot, Renaud De Landtsheer, Christophe Ponsard

CETIC a.s.b.l. • Bâtiment Eole • Rue des Frères Wright, 29/3 • B-6041 Charleroi (Belgique) • T. +32 71 490 700 • F. +32 71 490 799 • info@cetic.be

cetic

Your connection to ICT research

Outline

- Introduction
- Legal Requirements of Privacy Protection
- Walloon Region's eHealth Platform
- OrBAC Model
- Case study
- Implementation
- Conclusions and Perspectives

cetic

Your connection to ICT research

Outline

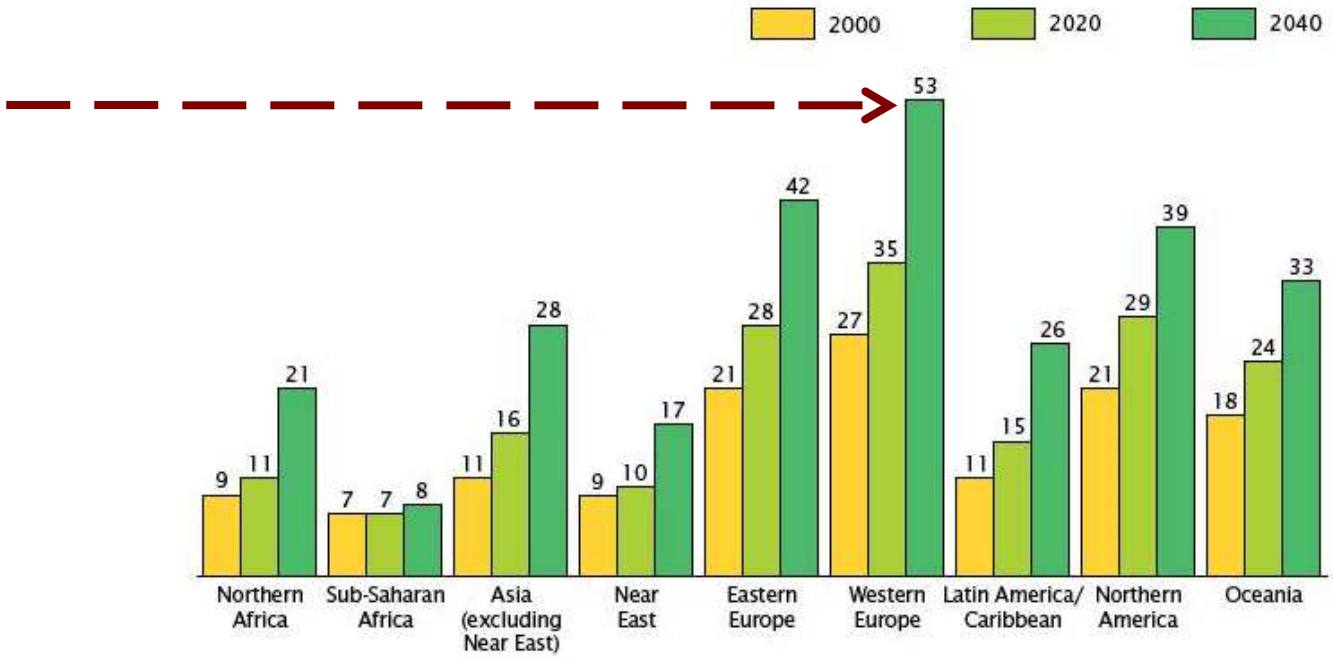
- Introduction
- Legal Requirements of Privacy Protection
- Walloon Region's eHealth Platform
- OrBAC Model
- Case study
- Implementation
- Conclusions and Perspectives

cetic
Your connection to ICT research

Aging Population

- Significant increase of elderly population especially in Europe

Figure 7-3.
Older Dependency Ratio for World Regions: 2000, 2020, and 2040



Note: Older dependency ratio is the number of people aged 65 and over per 100 people aged 20 to 64.
Source: U.S. Census Bureau, International Data Base, accessed on January 10, 2008.

Image taken from: K. Kinsella & W. He, An Aging World: 2008 – Int. Population Reports (P95/09-01), June 2009

cetic
Your connection to ICT research

Aging Population

- Elderly population will outnumber young children population by 2018

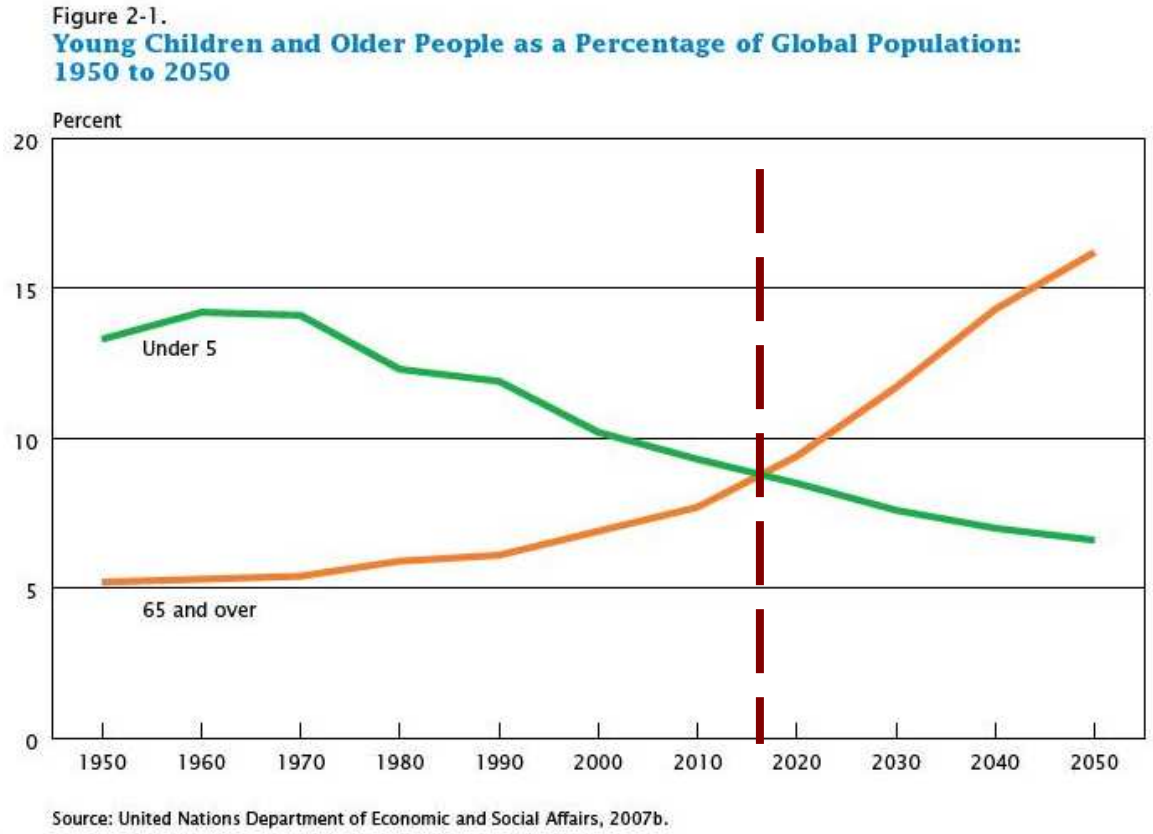


Image taken from: K. Kinsella & W. He, An Aging World: 2008 – Int. Population Reports (P95/09-01), June 2009

cetic
Your connection to ICT research

Elderly Population in Belgium

- Belgium is among the top 10 countries facing the increasing elderly population

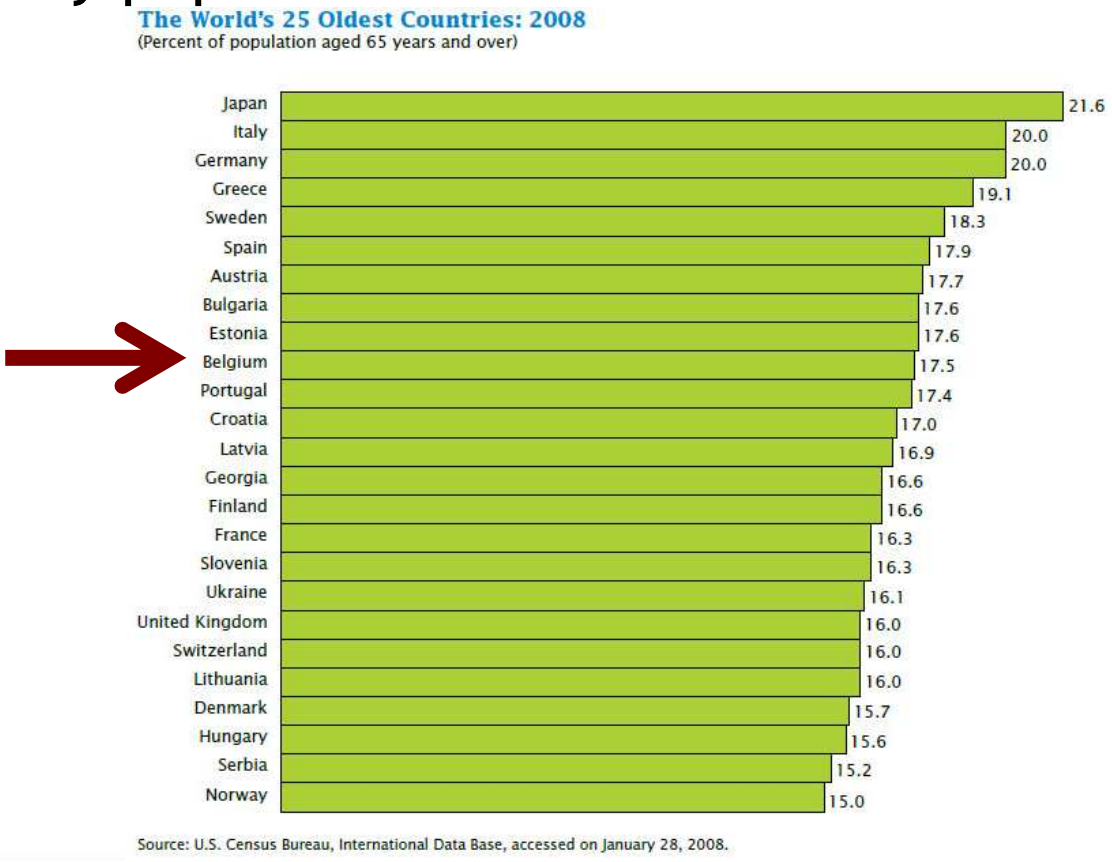


Image taken from: K. Kinsella & W. He, An Aging World: 2008 – Int. Population Reports (P95/09-01), June 2009

cetic
Your connection to ICT research

Health Issues of Elderly Population

- According to the estimates of Belgian National Statistical Institute: Elderly citizens will constitute one third of Belgium's population by 2060.
- Public bodies have to adapt their services for this demographic change.
- Health services will be overstretched due to increased medical care requirements of aging population and at the same time shortage of active workforce in the medical field.
- Non-traditional high-tech solutions are therefore indispensable to cope with this situation.

cetic

Your connection to ICT research

Outline

- Introduction
- Legal Requirements of Privacy Protection
- Walloon Region's eHealth Platform
- OrBAC Model
- Case study
- Implementation
- Conclusions and Perspectives

cetic
Your connection to ICT research

European Union Directive 95/46/EC

This directive sets the foundations of **confidentiality as fundamental principles** applicable to all forms of electronic communications. It imposes conditions of **transparency**, **legitimacy** and **proportionality** for the processing of personal data

Article 29 Data Protection Working Party

cetic
Your connection to ICT research

Belgian law on Privacy Protection

- Article 22 of the Belgian Constitution
  - guarantees the right of privacy & private communications
- Belgian Data Protection Act of 1992
  - to regulate the processing and use of personal information
- This legislation was subsequently modified
  - to make it coherent with the European directive 95/46/EC
- The definition of ***processing*** is extended in the new law
  - to enlarge the scope of its application
  - to determine the possible processing of special categories of data
  - to reinforce data subjects' rights

Legal Issues for the eHealth Platform

- The collection, storing, and processing of data over the eHealth Platform requires strict adherence to the **legal legislations**.
- The project consortium includes interdisciplinary experts of IT laws to assure the compliance of legal and regulatory issues.
  - Two main requirements are emerging from this law:
    - The access must be compliant with the finality of the collected private data
    - The collected data must be proportional to the finality

It implies that the access must be as restrictive as possible depending of the access finality. So, the access context has to be considered in order to determine the finality. The context has a direct impact on rights.

cetic

Your connection to ICT research

Outline

- Introduction
- Legal Requirements of Privacy Protection
- Walloon Region's eHealth Platform
- OrBAC Model
- Case study
- Implementation
- Conclusions and Perspectives

cetic
Your connection to ICT research

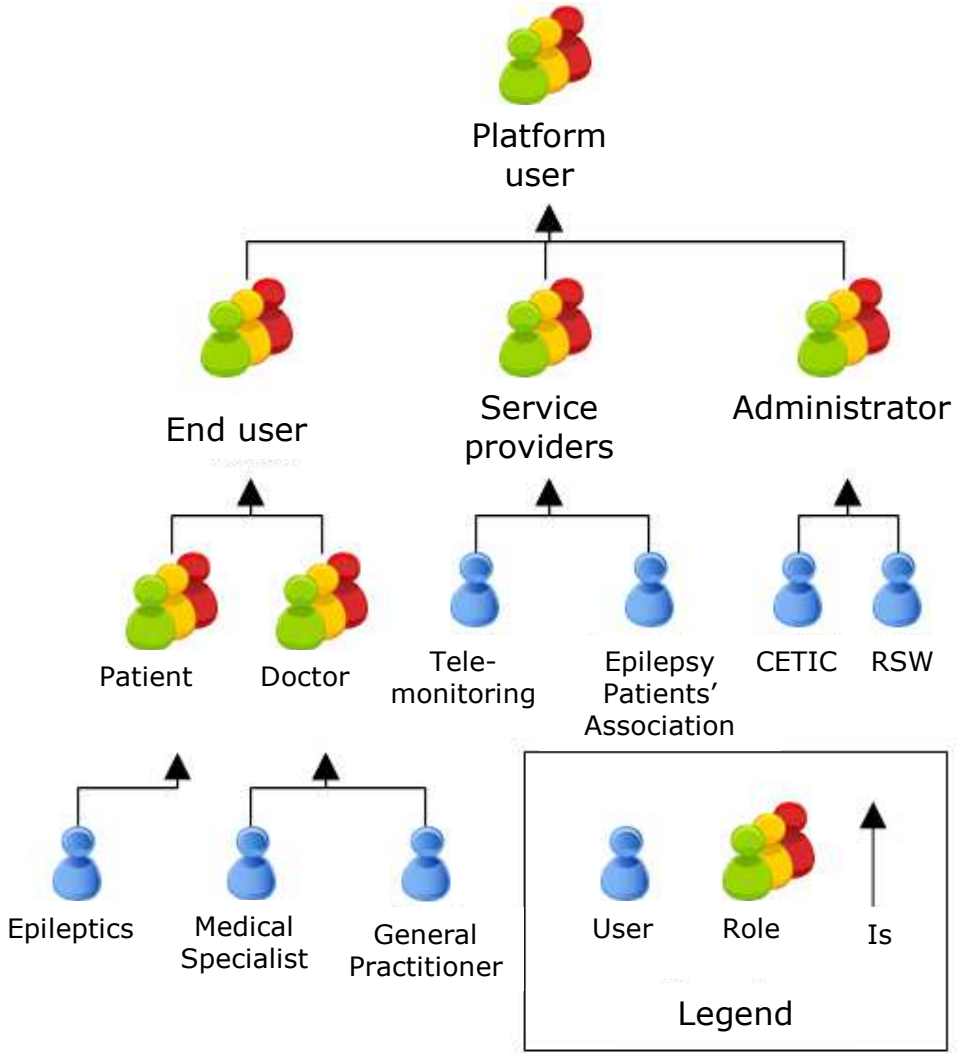
eHealth Platform Project

eHealth - les TIC au service des patients

- Funded by the Belgian Walloon Region
- CETIC : Project coordinator
- Other project partners include
  - University Hospital of Charleroi
  - Association of General Practitioners
  - Patients Association
  - Health Insurance Companies
  - Universities: UCL, FUNDP
  - Research Centres: ImmuneHealth, MULTITEL, CETIC
  - Public bodies: RSW, RW, SPF
- Initially 3 groups of beneficiaries
  - Elderly citizens
  - Epilepsy patients
  - Parkinson patients

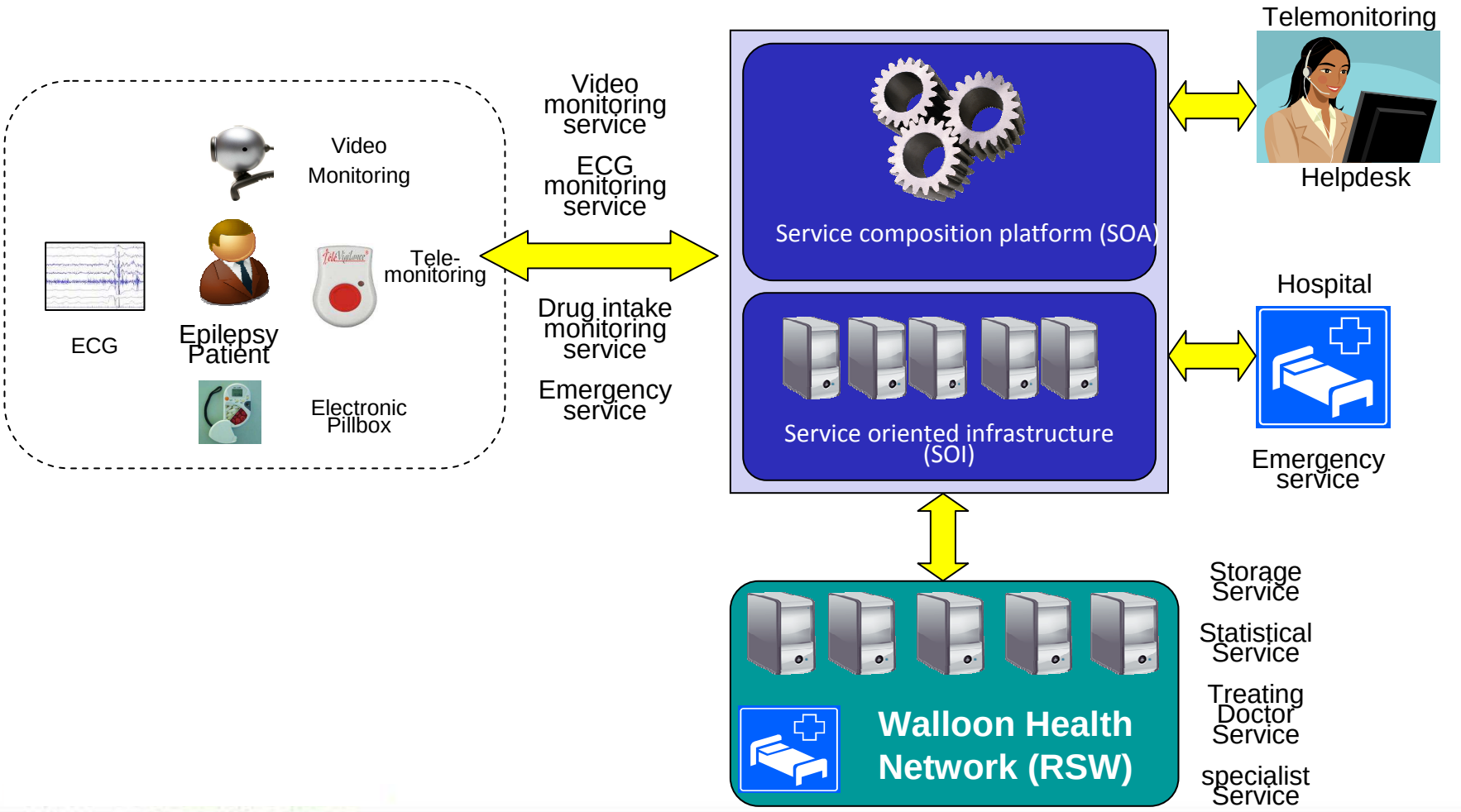
cetic
Your connection to ICT research

eHealth Platform's Stakeholders



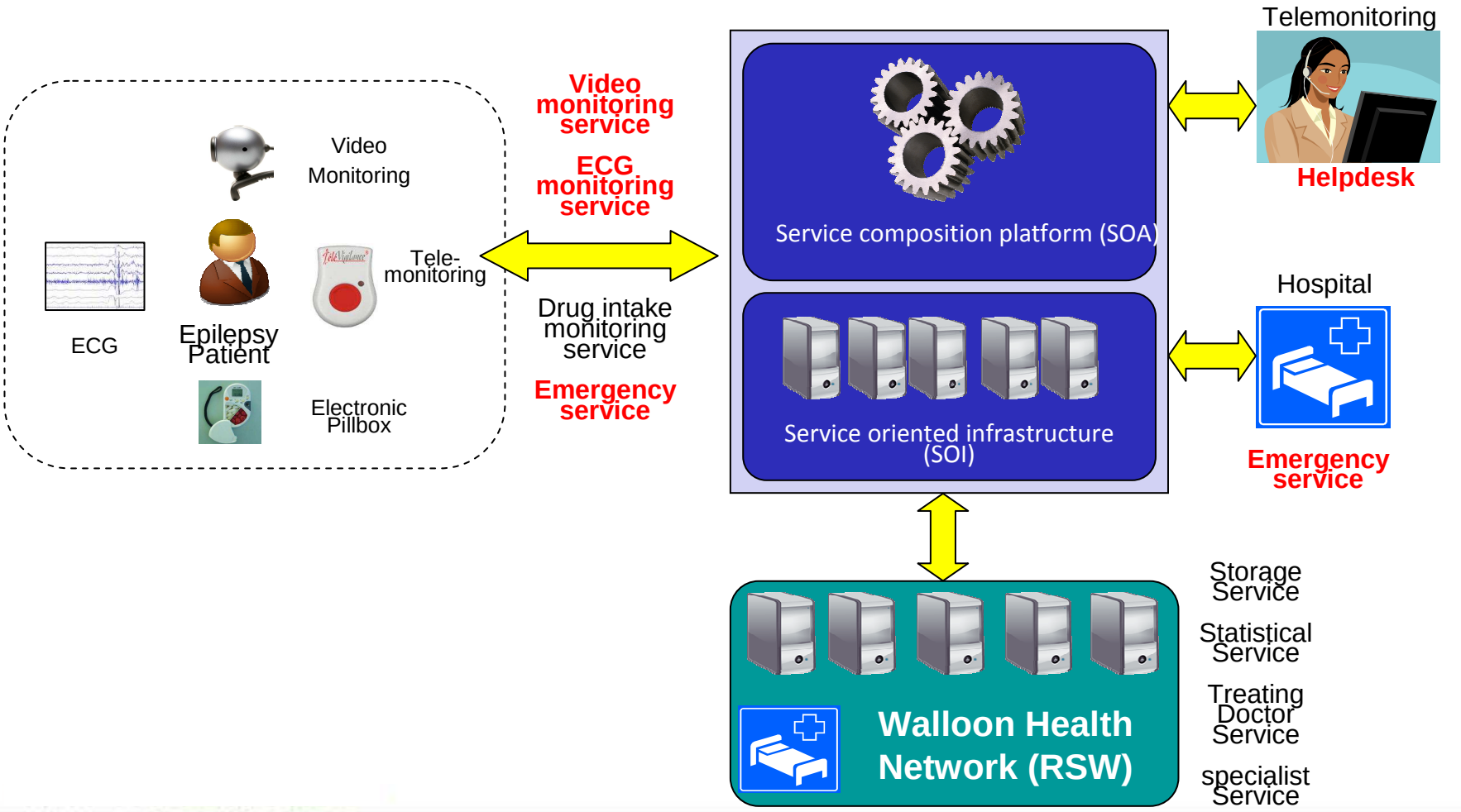
cetic
Your connection to ICT research

Example scenario: Monitoring of Epilepsy Patients



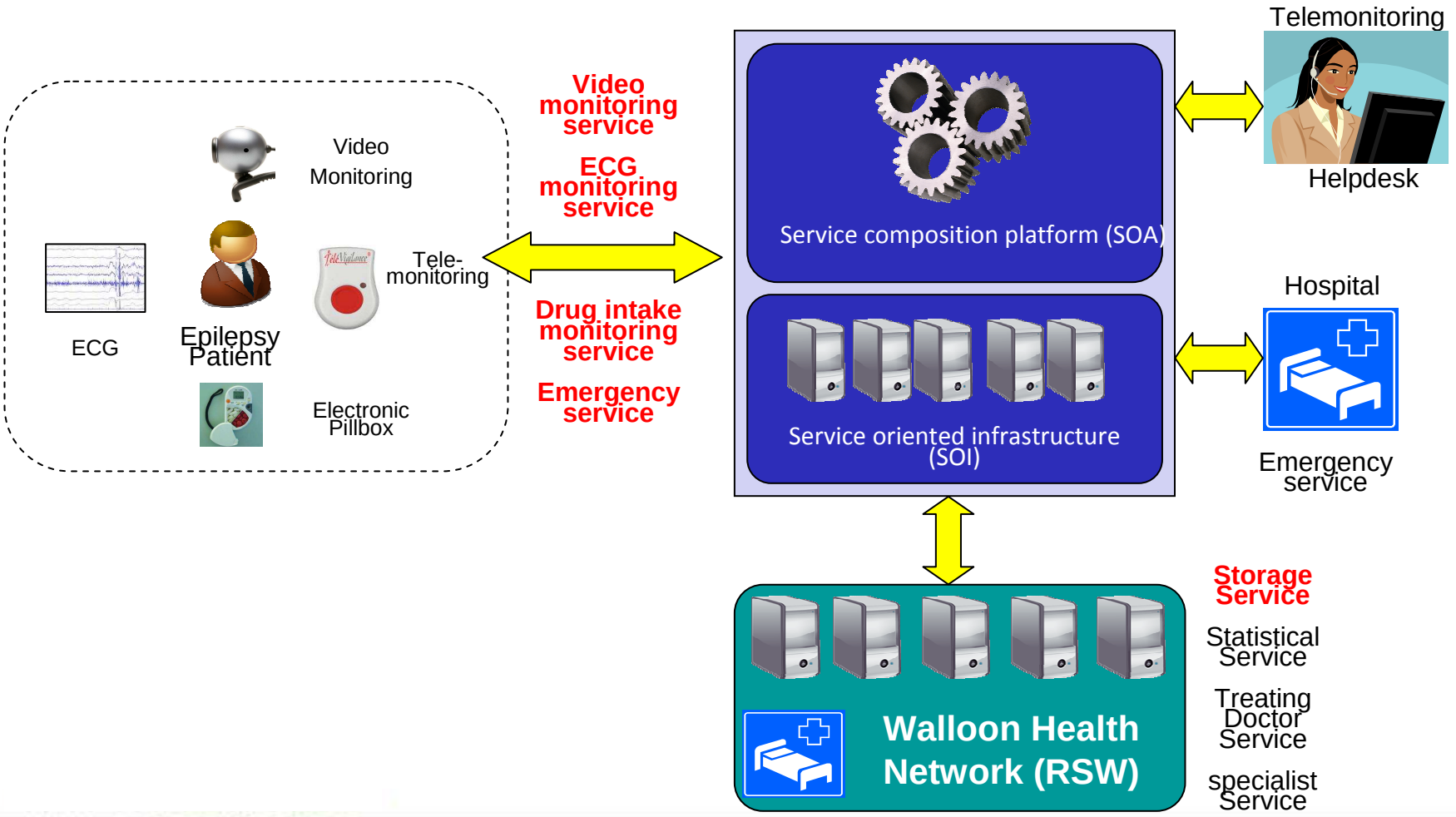
cetic
Your connection to ICT research

Example scenario: Monitoring of Epilepsy Patients



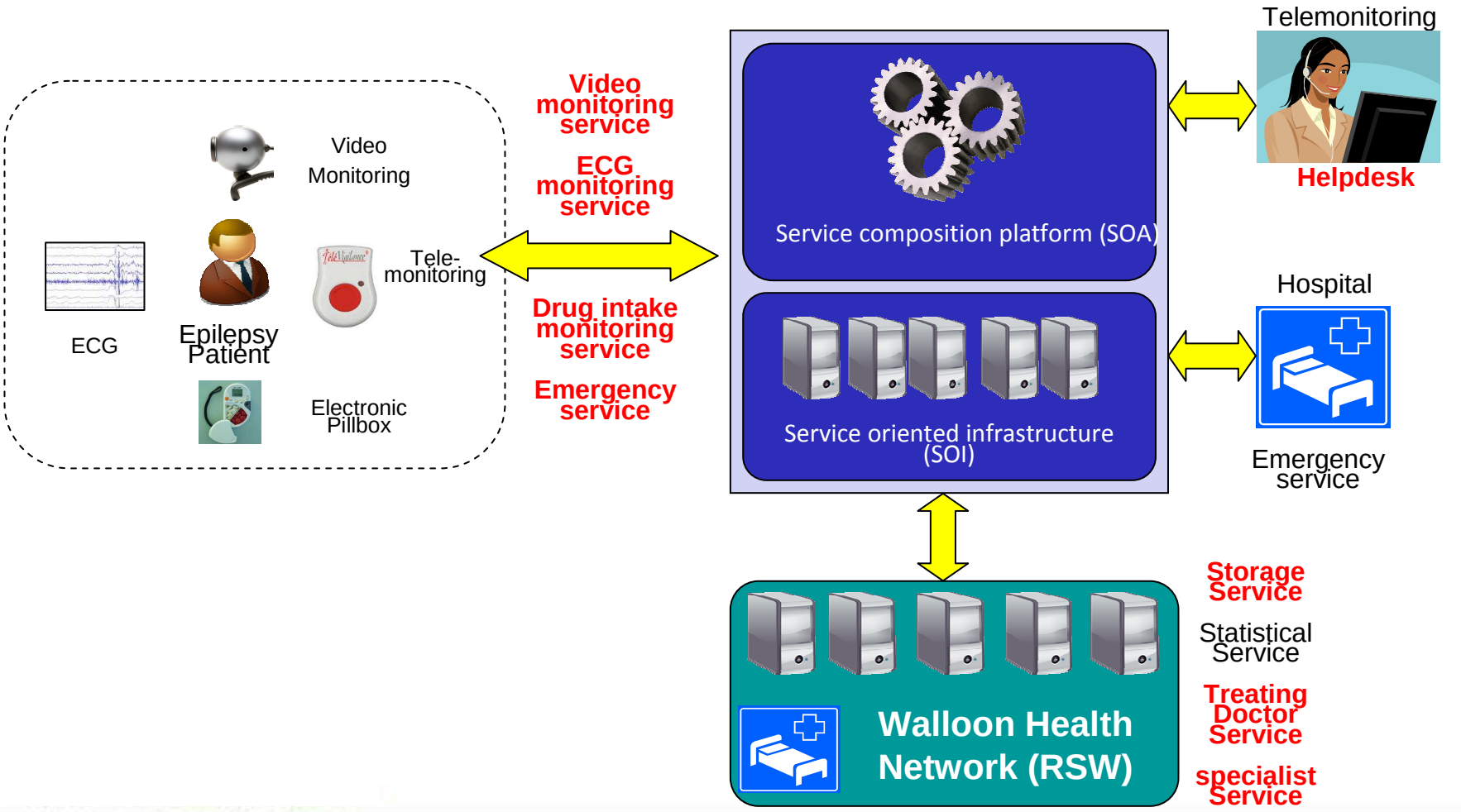
cetic
Your connection to ICT research

Example scenario: Monitoring of Epilepsy Patients



cetic
Your connection to ICT research

Example scenario: Monitoring of Epilepsy Patients



cetic

Your connection to ICT research

Outline

- Introduction
- Legal Requirements of Privacy Protection
- Walloon Region's eHealth Platform
- OrBAC Model
- Case study
- Implementation
- Conclusions and Perspectives

cetic
Your connection to ICT research

Access Control

- Different techniques for defining access control policies
  - Access Control Lists (ACL)
  - Discretionary Access Control (DAC)
  - Mandatory Access Control (MAC)
  - Role-based Access Control (RBAC)
  - Organization-based Access Control (OrBAC)
  - Bell-LaPadula Confidentiality Model
  - Biba Integrity Model
  - Chinese Wall Model

- **OrBAC is chosen for the eHealth Platform**

cetic
Your connection to ICT research

OrBAC Model

- OrBAC model allows security policy definition independent of its implementation details by introducing an abstract level.
- The granularity of the policy definition is at the organization level and therefore abstraction is done via the organization.
- Another interesting feature of OrBAC is its capacity to handle dynamic security policies by using contexts
  - temporal context, spatial context, user-declared context, prerequisite context, provisional context.
- This model is the only one making possible to implement requirements emerging from privacy law.
- It allows dynamic right depending on access context.

cetic

Your connection to ICT research

OrBAC Model

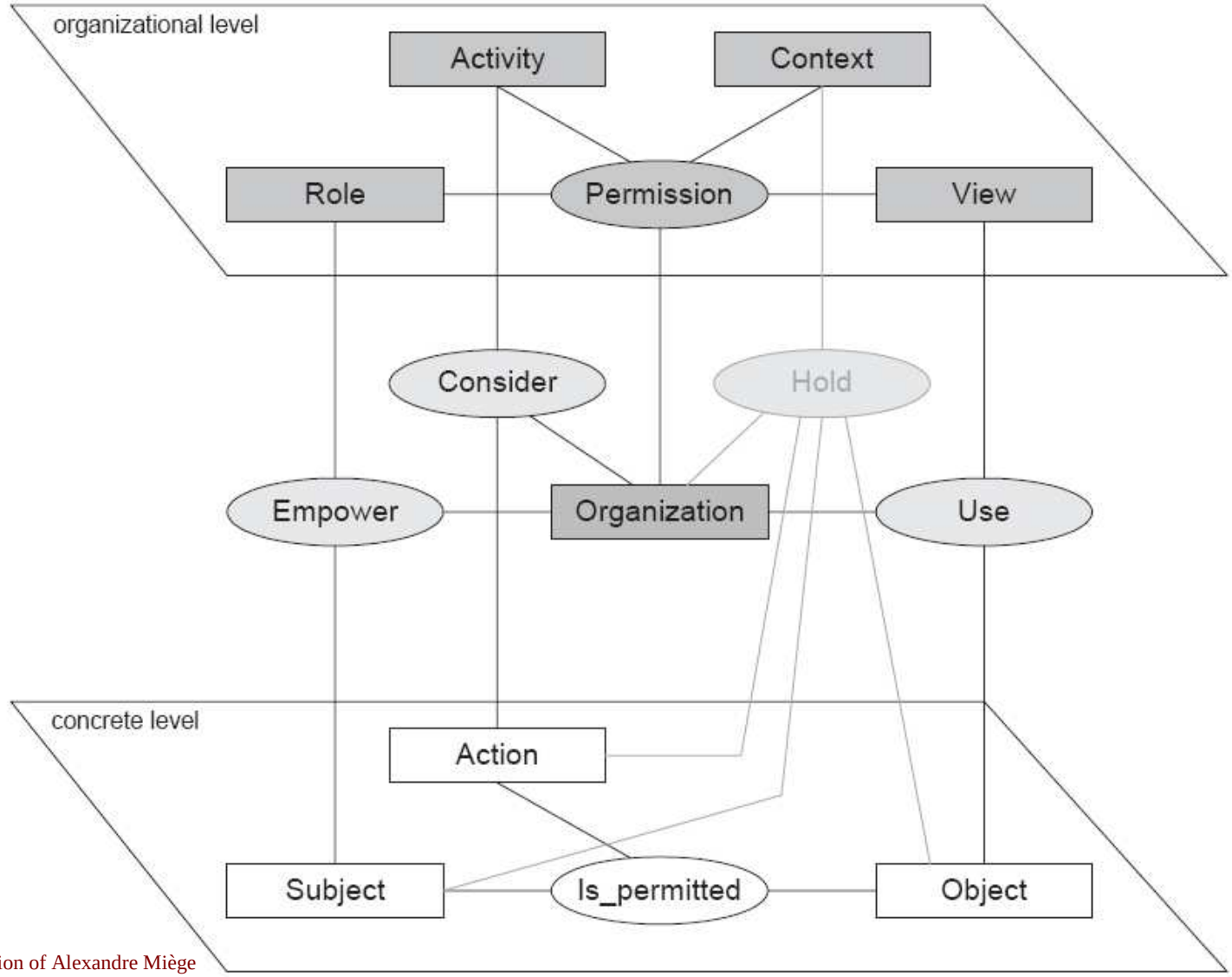


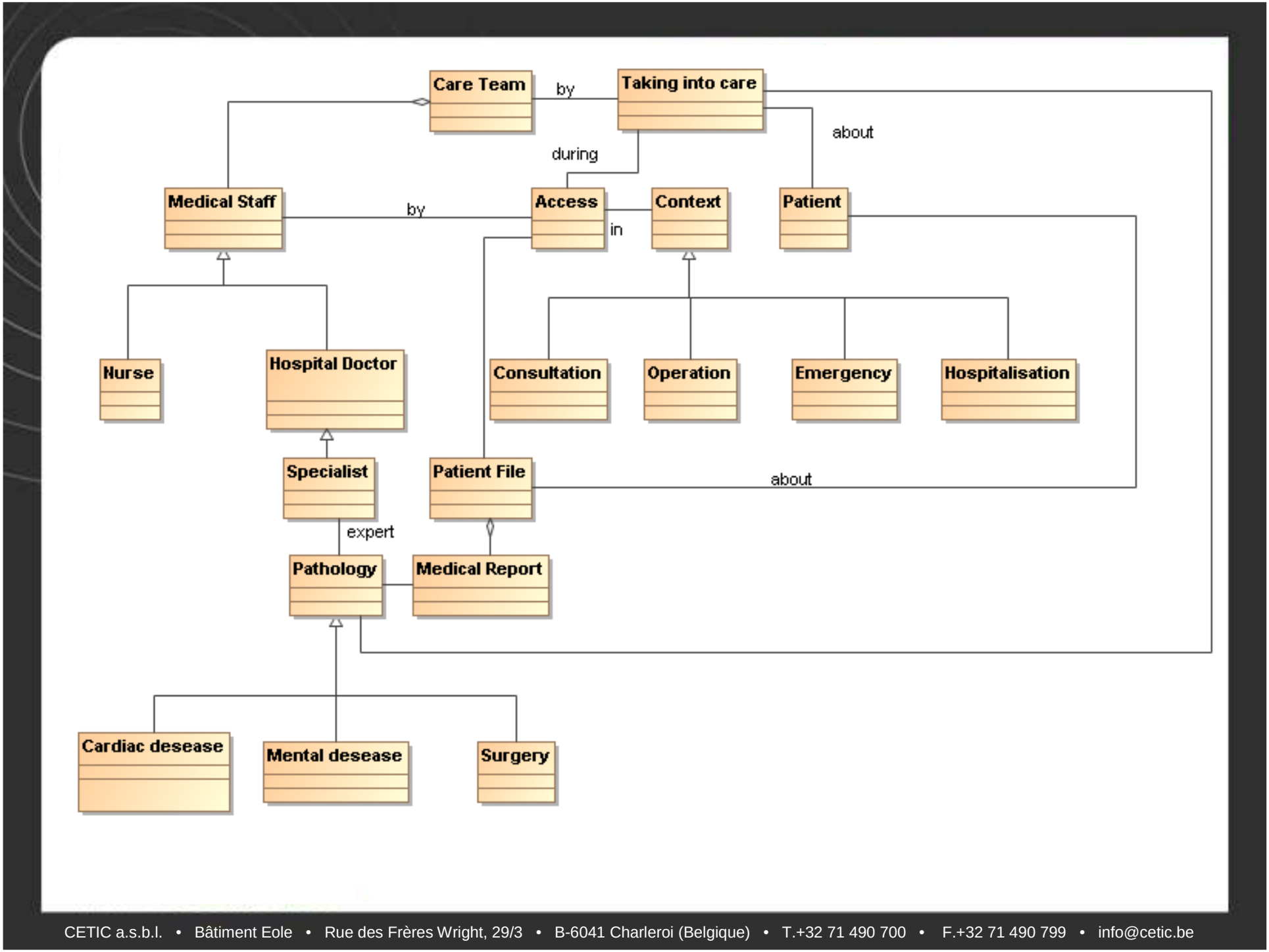
Image taken from the PhD dissertation of Alexandre Miège

cetic

Your connection to ICT research

Outline

- Introduction
- Legal Requirements of Privacy Protection
- Walloon Region's eHealth Platform
- OrBAC Model
- Case study
- Implementation
- Conclusions and Perspectives


Care Team
by
Taking into care
about
during
Medical Staff
by
Access
Context
in
Patient
Nurse
Hospital Doctor
Consultation
Operation
Emergency
Hospitalisation
Specialist
Patient File
about
expert
Pathology
Medical Report
Cardiac desease
Mental desease
Surgery

cetic
Your connection to ICT research

Dynamic Rights Management

- As a general rule, doctors only have access to their specialty if they take care of the patient except in specific contexts.
- In consultation only physicians who are responsible have access to the part of the record concerning (a cardiologist, the cardiac record, ...)
- In operation, the entire team of care access to the file (including nurses) except psychiatric records.
- In any emergency team to support access to everything.
- In the hospital, only doctors who take care have access to the entire medical record except the psychiatric.

cetic
Your connection to ICT research

The Invariants

- All medical staff have access to health records in emergency situations.
- The psychiatric record is accessible only to the psychiatrist who takes care of the patient except in an emergency situation.
- The nurses never have access to medical records except in emergency situations or in the operation theatre where doctors are already present.
- Only the doctor who is treating a patient have access to the patient's medical records (partial or total depending on the situation).

cetic

Your connection to ICT research

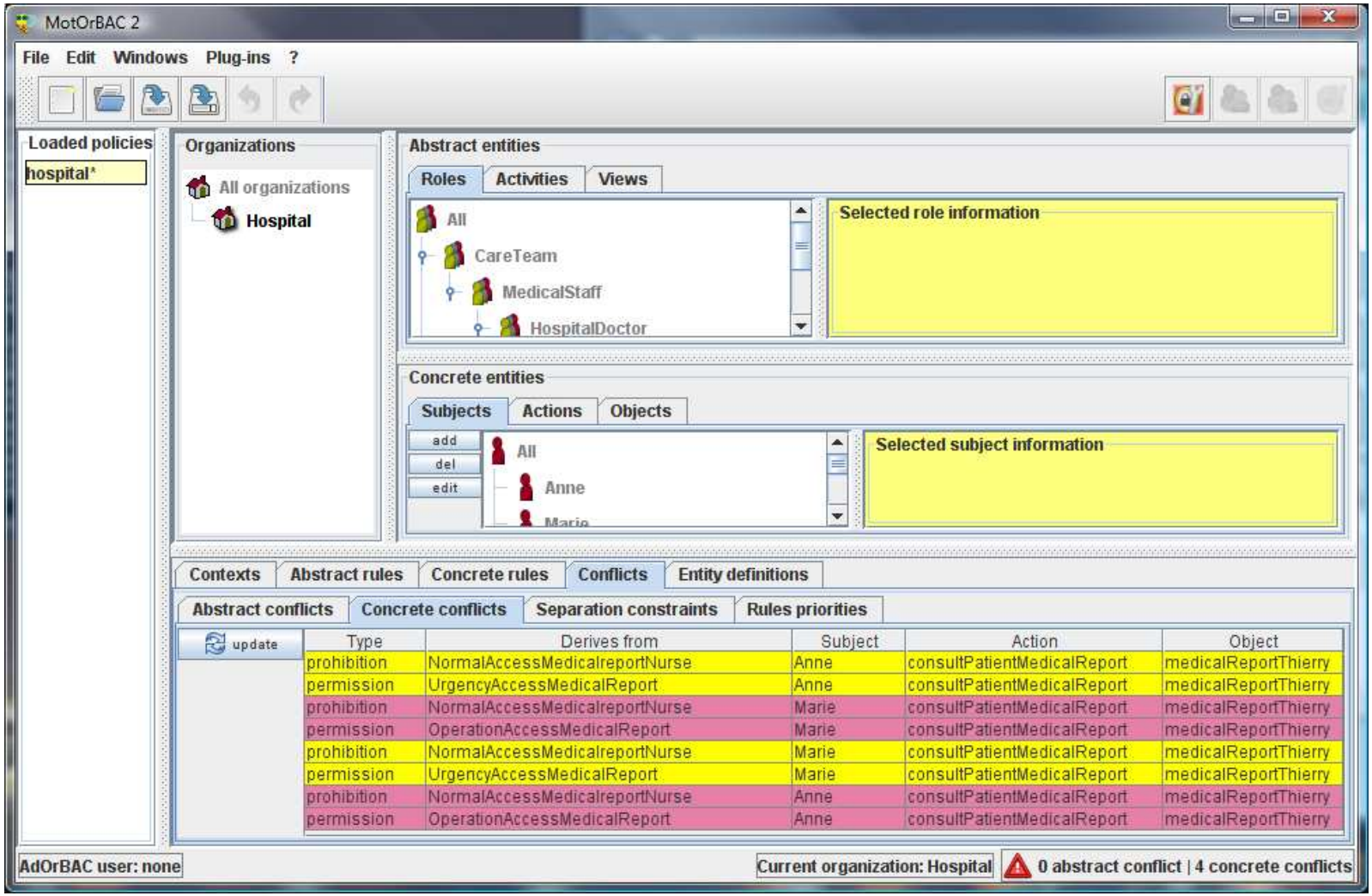
Outline

- Introduction
- Legal Requirements of Privacy Protection
- Walloon Region's eHealth Platform
- OrBAC Model
- Case study
- **Implementation**
- Conclusions and Perspectives

cetic

Your connection to ICT research

MotOrBAC



cetic

Your connection to ICT research

Outline

- Introduction
- Legal Requirements of Privacy Protection
- Walloon Region's eHealth Platform
- OrBAC Model
- Case study
- Implementation
- Conclusions and Perspectives

cetic
Your connection to ICT research

Conclusions

- The eHealth project of Belgian Walloon region is an ambitious initiative
  - aims to address the growing needs of contemporary healthcare practices
- The emerging technology-based public healthcare systems offer promising feature of ensuring needful healthcare facilities to the population
  - especially to the increasing proportion of society's elderly population
- Technology-based healthcare solutions such as telemedicine have already been striving for some comprehensible solutions for assuring the privacy of personal data
- These systems have to be equipped with the adequate security features
  - to provide privacy assurances to comply with legal obligations.

cetic
Your connection to ICT research

Perspectives

- The features of eHealth platform can be extended to include electronic prescribing for assuring secure interoperability of eHealth medical records with its counterparts in other countries/regions.
- This work will require to workout the security requirements for assuring overall privacy in the advent of integrating the eHealth platform into a European or into some other international Healthcare infrastructure (such as Health-Grid).
- There is also the need to investigate the privacy concerns associated with the use of smart devices in the eHealth platform.
  - The security and privacy concerns are exacerbated when these gadgets are deployed in the open networking architectures. The term *internet of things* is recently coined for this paradigm.
- Our future directions include research on privacy assurance solutions for the eHealth platform composed over the internet of things.

cetic

RESERVOIR

Thank you

CETIC a.s.b.l. • Bâtiment Eole • Rue des Frères Wright, 29/3 • B-6041 Charleroi (Belgique) • T. +32 71 490 700 • F. +32 71 490 799 • info@cetic.be