EHEALTH FOR THE CITIZEN FOR BETTER PRIVACY AND DATA PROTECTION

Christos N. Schizas, Professor of Computer Science, University of Cyprus

Follow us @eHealthWeekEU #eHW15

eHealth week

11 - 13 MAY 2015
RIGA, LATVIA

ORGANISED BY

EU2015.LV

Ministry of Health
Republic of Latvia

meHEALTH

WHIT

eHealth for all

EHEALTH FOR THE CITIZEN FOR BETTER PRIVACY AND DATA PROTECTION

Follow us @eHealthWeekEU #eHW15

SOME OF THE KEY BENEFITS FOR PATIENTS ARE:

- Recognition for the **first time** in EU law that patients have a right to cross-border healthcare and are entitled to be reimbursed for it;
- **Right to information** on cross-border healthcare, and the creation of **National Contact Points** in each Member State to provide this;
- Right of patients to obtain a copy of their medical record and to get appropriate **medical follow-up in the home country;**
- **Recognition** of prescriptions made abroad ;
- **Transparency** on the quality and safety standards for healthcare that apply in each Member State;
- **Legal basis** for European co-operation on eHealth and Health Technology Assessment;
- **Better cooperation** between Member States in rare diseases, including establishing a legal basis for European Reference Networks and centres of excellence.

eReferral

Diagnostic Centres

Hospitals

Emergency Health Care

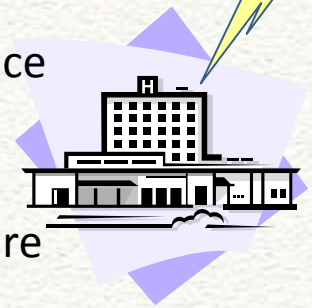
Home Care

Medical Databank

Medical Centres

General Practice

Medical Libraries



Citizen care

Multi-specialization centres

Health Kiosk

Pharmacy ePrescription

Personal Medical Record – Citizen Record

The citizens become **owners** of the data that concerns them.

With the capability of the system to:

- **Store** medical data from different sources
- **Store** medical data from medical devices
- **Access** from authorised personnel when needed to this data.

Security issues of eHealth Records (EHR)

- **Considering an EHR of a patient where:**
  - all medical record and history is maintained electronically
  - under his ownership (with his responsibility)
  - under the supervision of his doctors
  - on a cloud service provided by a third external partner.
- **Security Systems and Solutions for decades:**
  - **http://www.verisign.com/** secure purchasing on the web (SSL)
  - Authentication etc.

For this presentation skip slides 8-18

Security issues of eHealth Records

- ***Privacy-preserving data publishing* (PPDP)**; hospitals and governmental services may have to share due to research purposes or regulations such data. Data publishing of personal data needs to preserve privacy and sensitive data.
- ***Access Control of EHR*;** the EHR of a long medical history of the patient; various specialists should have different privilege accesses on parts of this data. For instance, the personal doctor (with the permission of the patient) may provide full access to a hematologist but limited access to a podiatrist.
- ***Cryptography***; Cryptography plays three major roles in the implementation of secure systems:

  Secrecy and integrity – Authentication - Digital signatures

All these facilities are necessary since data maybe maintained in 3rd parties and their remote access will be required.

Privacy-preserving data publishing (PPDP)

- Hospitals, Medical centers, etc. may have to share their data either for research purposes or due to regulations (eHealth).
- There is already a lot of research and practical solutions:
- ***k-Anonymity -*** A record is indistinguishable from at least *k*−1 other records with respect to *Quasi ID*. Consequently, the probability of linking a victim to a specific record through *Quasi ID* is at most 1/*k*.
- ***i-Diversity -*** requires every *QID* group to contain at least *l* "well-represented" sensitive values; e.g. ensure that there are at least *l* distinct values for the sensitive attribute in each QID group.
- Other PPDP: ***t-Closeness, FF-Anonymity, δ-Presence***

Privacy-preserving data publishing (PPDP)

Job	Sex	Age	Disease
Engineer	Male	35	Hepatitis
Engineer	Male	38	Hepatitis
Lawyer	Male	38	HIV
Writer	Female	30	Flu
Writer	Female	30	HIV
Dancer	Female	30	HIV
Dancer	Female	30	HIV

Job	Sex	Age	Disease
Professional	Male	[35-40)	Hepatitis
Professional	Male	[35-40)	Hepatitis
Professional	Male	[35-40)	HIV
Artist	Female	[30-35)	Flu
Artist	Female	[30-35)	HIV
Artist	Female	[30-35)	HIV
Artist	Female	[30-35)	HIV

Name	Job	Sex	Age
Alice Ho	Writer	Female	30
Bob Alan	Engineer	Male	35
Cathy Smith	Writer	Female	30
Doug Brown	Lawyer	Male	38
Emily Farthing	Dancer	Female	30
Fred Bishop	Engineer	Male	38
Gladys Macey	Dancer	Female	30
Henry Kassie	Lawyer	Male	39
Irene Ladybird	Dancer	Female	32

(PPDP): k-anonymity

Medical data

Names	Job	Sex	Age	Disease
Bob Alan	Engineer	Male	35	Hepatitis
Fred Bishop	Engineer	Male	38	Hepatitis
Doug Brown	Lawyer	Male	38	HIV
Cathy Smith	Writer	Female	30	Flu
Alice Ho	Writer	Female	30	HIV
Gladys Macey	Dancer	Female	30	HIV
Emily	Dancer	Female	30	HIV

Medical data after removing patients' names

Names	Job	Sex	Age	Disease
?	Engineer	Male	35	Hepatitis
?	Engineer	Male	38	Hepatitis
?	Lawyer	Male	38	HIV
?	Writer	Female	30	Flu
?	Writer	Female	30	HIV
?	Dancer	Female	30	HIV
?	Dancer	Female	30	HIV

Public, open dataset (e.g. Voters list)

Name	Job	Sex	Age
Alice Ho	Writer	Female	30
Bob Alan	Engineer	Male	35
Cathy Smith	Writer	Female	30
Doug Brown	Lawyer	Male	38
Emily Farthing	Dancer	Female	30
Fred Bishop	Engineer	Male	38
Gladys Macey	Dancer	Female	30
Henry Kassie	Lawyer	Male	39
Irene Ladybird	Dancer	Female	32

By simply removing names, an open dataset can still disclose patients' ID

Privacy-preserving data publishing (PPDP): k-anonymity

Medical data after removing patients' names

Job	Sex	Age	Disease
Engineer	Male	35	Hepatitis
Engineer	Male	38	Hepatitis
Lawyer	Male	38	HIV
Writer	Female	30	Flu
Writer	Female	30	HIV
Dancer	Female	30	HIV
Dancer	Female	30	HIV

Job	Sex	Age	Disease
Professional	Male	[35-40)	Hepatitis
Professional	Male	[35-40)	Hepatitis
Professional	Male	[35-40)	HIV
Artist	Female	[30-35)	Flu
Artist	Female	[30-35)	HIV
Artist	Female	[30-35)	HIV
Artist	Female	[30-35)	HIV

Public, open dataset (e.g. Voters list)

Name	Job	Sex	Age
Alice	Writer	Female	30
Bob	Engineer	Male	35
Cathy	Writer	Female	30
Doug	Lawyer	Male	38
Emily	Dancer	Female	30
Fred	Engineer	Male	38
Gladys	Dancer	Female	30
Henry	Lawyer	Male	39
Irene	Dancer	Female	32

{Lawyer, *Male*, 38}→ *HIV*
Thus, Doug has HIV

3-anonymous table by generalizing *QID={Job, Sex, Age}*.
E.g. {Professional, Male, [35-40)} at least 3

Privacy-preserving data publishing (PPDP): i-diversity

Medical data after removing patients' names

Job	Sex	Age	Disease
Engineer	Male	35	Hepatitis
Engineer	Male	38	Hepatitis
Lawyer	Male	38	HIV
Writer	Female	30	Flu
Writer	Female	30	HIV
Dancer	Female	30	HIV
Dancer	Female	30	HIV

Public, open dataset (e.g. Voters list)

Name	Job	Sex	Age
Alice	Writer	Female	30
Bob	Engineer	Male	35
Cathy	Writer	Female	30
Doug	Lawyer	Male	38
Emily	Dancer	Female	30
Fred	Engineer	Male	38
Gladys	Dancer	Female	30
Henry	Lawyer	Male	39
Irene	Dancer	Female	32

all female dancers at age 30 have *HIV*,
Dancer, Female,* 30}→ *HIV
Thus, Emily has HIV

***According to L-diversity, for {Dancer, Female,* 30} we should have at least l deceases rather only HIV**

Access Control of EHR

- According to the literature, there are different implementations of access control policies for determining the access that subjects may have on objects:
  - ***discretionary***,
  - ***mandatory***, and
  - ***role-based***.
- In such systems, there are two major components:
  - the **subjects** who take actions (in the EHR project, the subjects can be the patient and the medical staff) and
  - the **objects** they take actions on (namely, the various parts of this EHR).
- Access control policies specify the conditions under which a subject is allowed to take an action on an object.

Access Control of EHR

Role-Based Access Control (RBAC).

- Subjects assigned to roles that line up with roles that users hold in real life.
- A role could represent a set of actions and responsibilities that a subject has. For example, the patient, the personal doctor, a specialist, etc.
- The patient may have a full read access to his record but may not have the privilege to authorize doctors to have access on his EHR.
- His personal doctor may have full read access and also full privileges in allowing other doctors read-accessing parts of the EHR.
- In an EHR system, various roles would be created that represent different levels of access.
- Then, subjects in the system would be placed in their appropriate roles and each object authorizes access based on these roles.
- This type of system has many benefits. Management of authorizations is simplified since it is broken into the two separate tasks of assigning rights to roles, then assigning subjects to roles.

Cryptography

- **Secrecy and Integrity**
- Cryptography is used to maintain the secrecy and integrity of information whenever it is exposed to potential attacks;
- For example, during the storage on a cloud or during transmission across networks that are vulnerable to eavesdropping and message tampering.
  - **military and intelligence activities**
  - **encryption key**
  - **decrypted by the owner or the recipient**
  - **encryption algorithm is strong enough to defeat any possible attempts to crack it**.
- For instance, in the EHR context, the EHR is encrypted and the cloud provider cannot decrypt it.

Cryptography

- **Authentication**
- Cryptography is used in support of mechanisms for authenticating communication between pairs of principals.
  - **can assume that the message is authentic if it contains a correct checksum or some other expected value.**
  - **if keys are held in private, a successful decryption authenticates the decrypted message as coming from a particular sender.**
- For instance, a doctor wishes to access files held by a cloud server.
  - **Another third party (e.g. *www.verisign.com*) is an authentication server.**
  - **is securely managed and issues users with passwords.**
  - **holds current secret keys for all of the principals in the system it serves.**
  - **it knows doctor and cloud server's keys.**

Cryptography

Digital signatures

- Cryptography is used to implement a mechanism known as a ***digital signature*.**
- Digital signature techniques are based upon an irreversible binding to the message or document of a secret known only to the signer.
- This can be achieved by encrypting the message, or better, a compressed form of the message called a ***digest***, using a key that is known only to the signer.
- Public-key cryptography is generally used for this
  - **the originator generates a signature with their private key**.
  - **the signature can be decrypted by any recipient using the corresponding public key**.
  - **the verifier should be sure that the public key really is that of the principal claiming to be the signer.**
- For instance, a specialist wants to sign a medical report of a patient
  - **any subsequent recipient can verify that he is the originator of it**.
  - **when other medical staff later accesses the signed document after receiving it by any route and from any source.**
  - **they can verify that the specific specialist is the originator.**

Funded research projects of the eHealth Lab of the University of Cyprus on Security

- **fi-star** -Future Internet Social and Technological Alignment Research. Electronic Health Record Application Support Service Enablers (EHR-EN). Funded by EU. www.fi-star.eu

- **Linked2Safety** -A Next-Generation, Secure Linked Data Medical Information Space For Semantically-Interconnecting Electronic Health Records. www.linked2safety-project.eu

Funded research projects of the eHealth Lab of the University of Cyprus on Security

- e-ENERCA-Towards an eHealth based European Reference Network. Funded by EU. Focus on eHealth tools for rare anaemias. www.enerca.org/activities-news/news/69/enerca-enters-a-new-era-e-enerca

European Network for Rare and Congenital Anaemias

Work Package 4

EUROPEAN EPIDEMIOLOGICAL SURVEILLANCE FOR MAJOR RARE ANAEMIAS

Aims

Creation of a registry service comprised :

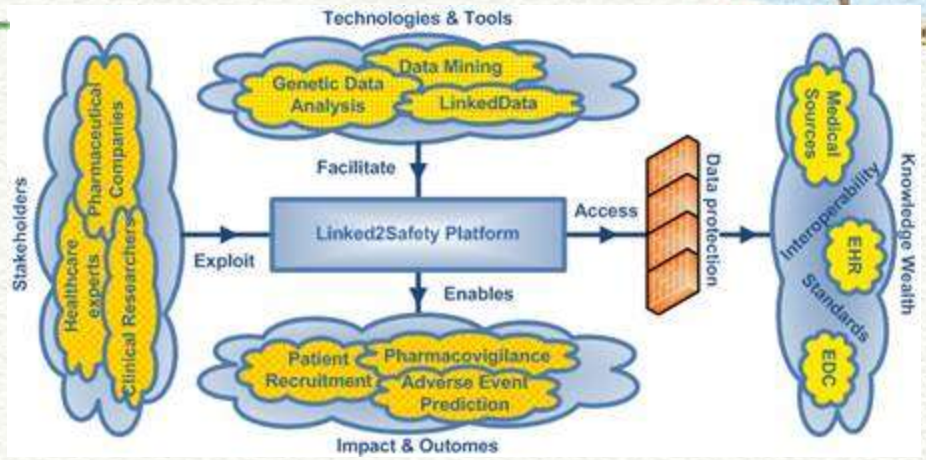
a) Front-end service including the functionality of filling-in on line forms for acquiring epidemiological data and retrieving the data in a report format.

b) Database and DBMS that stores and maintains the health information records in EHR format. Thus a pan-European interoperable Registry for major Rare Anaemias and other epidemiological health records will be created.

Linked2Safety

- A Next-Generation, Secure Linked Data Medical Information Space For Semantically-Interconnecting Electronic Health Records and Clinical Trials Systems Advancing Patients Safety In Clinical Research.

project

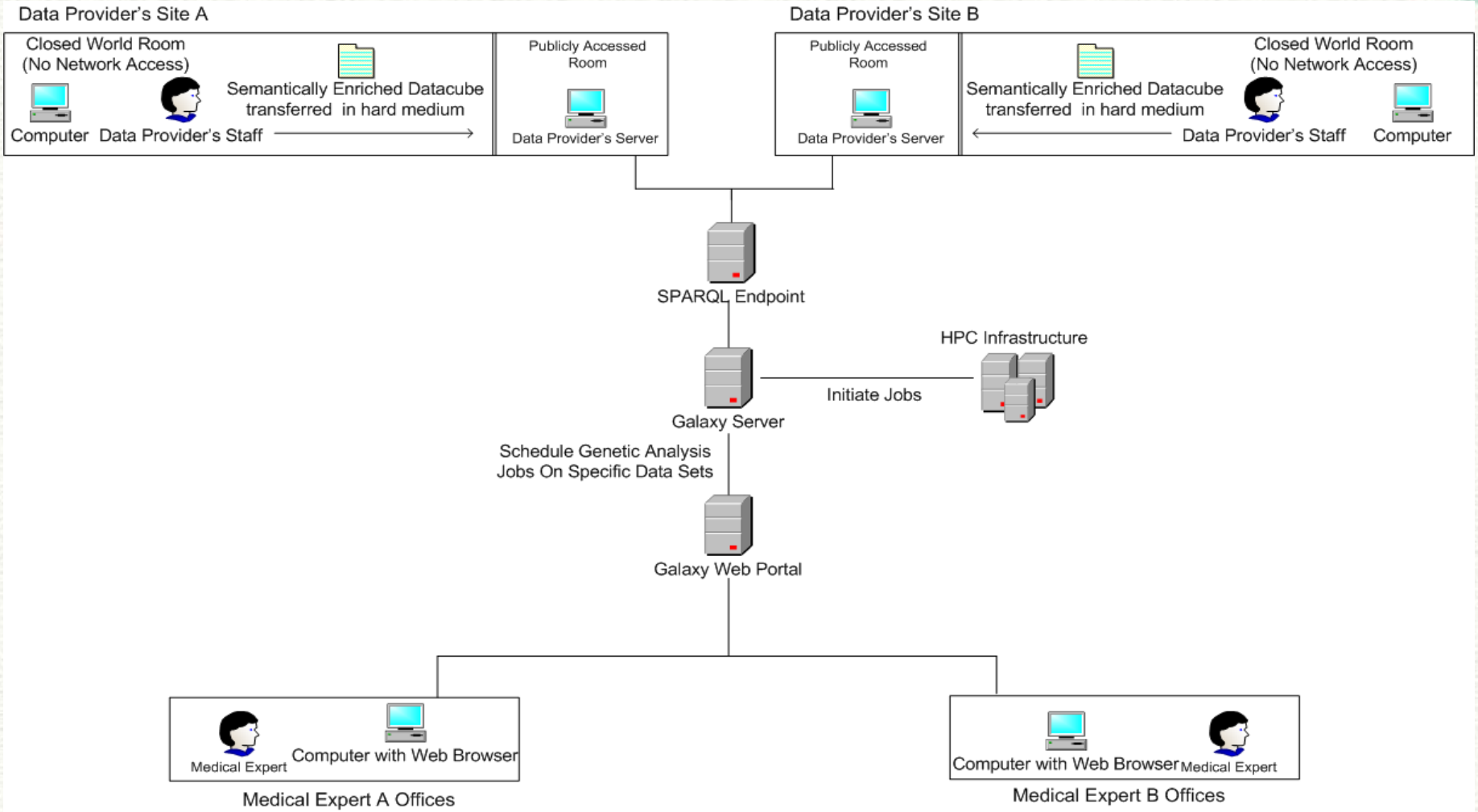


- The vision
  - Ensure and empower patients' safety, supporting clinical and medical research and improving the quality of healthcare
  - by providing patients, healthcare professionals and pharmaceutical companies
    - with an innovative interoperability framework
    - a sustainable business model
    - a scalable technical infrastructure and platform for the efficient, homogenized access to and the effective utilization of the increasing wealth of medical information contained in the Electronic Health Records (EHRs) systems deployed and maintained at regional and/or national level across Europe,
  - by dynamically interconnecting distributed patients data with clinical research efforts, respecting patients' anonymity, data ownership and privacy, as well as European and national legislation.

Linked2Safety : A secure linked data medical information space

- Enables the joint analyses of medical data across multiple sites in Europe through the power of aggregation and data mining **to handle legal and ethical issues**.
- Design and develop the data mining techniques and the scalable infrastructure for large scale multi-center pharmacovigilance trials.
- Develop new and implement existing state of the art analytical approaches for genetic data taking advantage of the explosion in –omic analytics used in the clinical setting.
- Define and implement the knowledge extraction and filtering mechanisms and the knowledge base
- Integrate the knowledge base into a lightweight decision support system (Adverse events early detection mechanism)

Linked2Safety Architecture

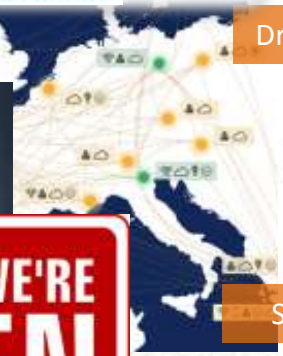


Understanding FIWARE

(Open Standard Platform)

(Advanced OpenStack-based Cloud + rich library of Enablers)

FIWARE
OPEN APIs FOR OPEN MINDS



Driven by implementation

Sustainability ensured

eHealth week 11 - 13 MAY 2015 RIGA, LATVIA

Follow us @eHealthWeekEU #eHW15

FIWARE enablers ecosystem features

36 Generic enablers

And Specific enablers

Cloud		• Federation of infrastructures (private/public regions) • Automated GE deployment
Data/Services Delivery		• Complete Context Management Platform • Integration of Data and Media Content
IoT		• Easy plug&play of devices using multiple protocols • Automated Measurements/Action - Context updates
Apps		• Visualization of data (operation dashboards) • Publication of data sets/services
Web UI		• Easy incorporation of advanced 3D and AR features • Visual representation of context information
Security		• Security Monitoring • Built-in Identity/Access/Privacy Management
I2ND		• Advanced networking (SDN) and middleware • Interface to robots
FISTAR	fistar	• Health specific enablers • Data to applications paradigm

fistar

7 Use cases

Interoperability profiles

Requirements

Specific Enablers

Testing & validation

Tromsø, Norway

Tele-health network for Diabetes patients

Munich, Germany

Virtualization of operating theatre environments and real time dataintegration for monitoring and reduction of errors

Leeds, UK

2-D bar-coding for real time reverse medicament supply chain

Krakow, Poland

Interactive online facilities for accessand quality of care

Bilbao, Spain

New Interactive Future Internet based services for people with Mental Health problems

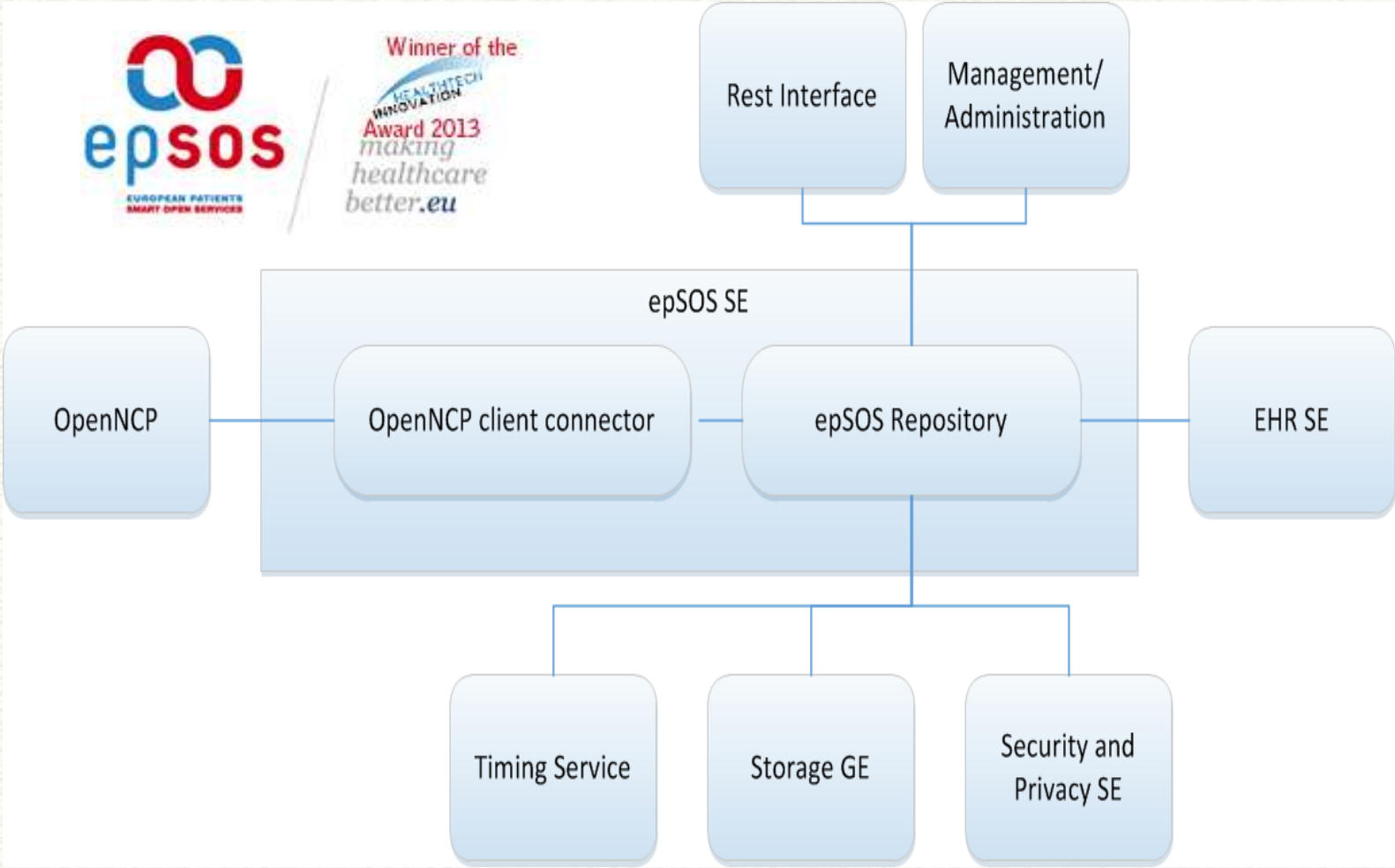
Bucharest, Romania

Online Cardiology service for people with heart failure

Bologna, Italy

Provision of a network capable to connect different applications and devices

The epSOS SE architecture - interdependency between the FI-STAR and FI-WARE platforms



IHE EUROPE CONNECTATHON

LUXEMBOURG APRIL 20-24 2015

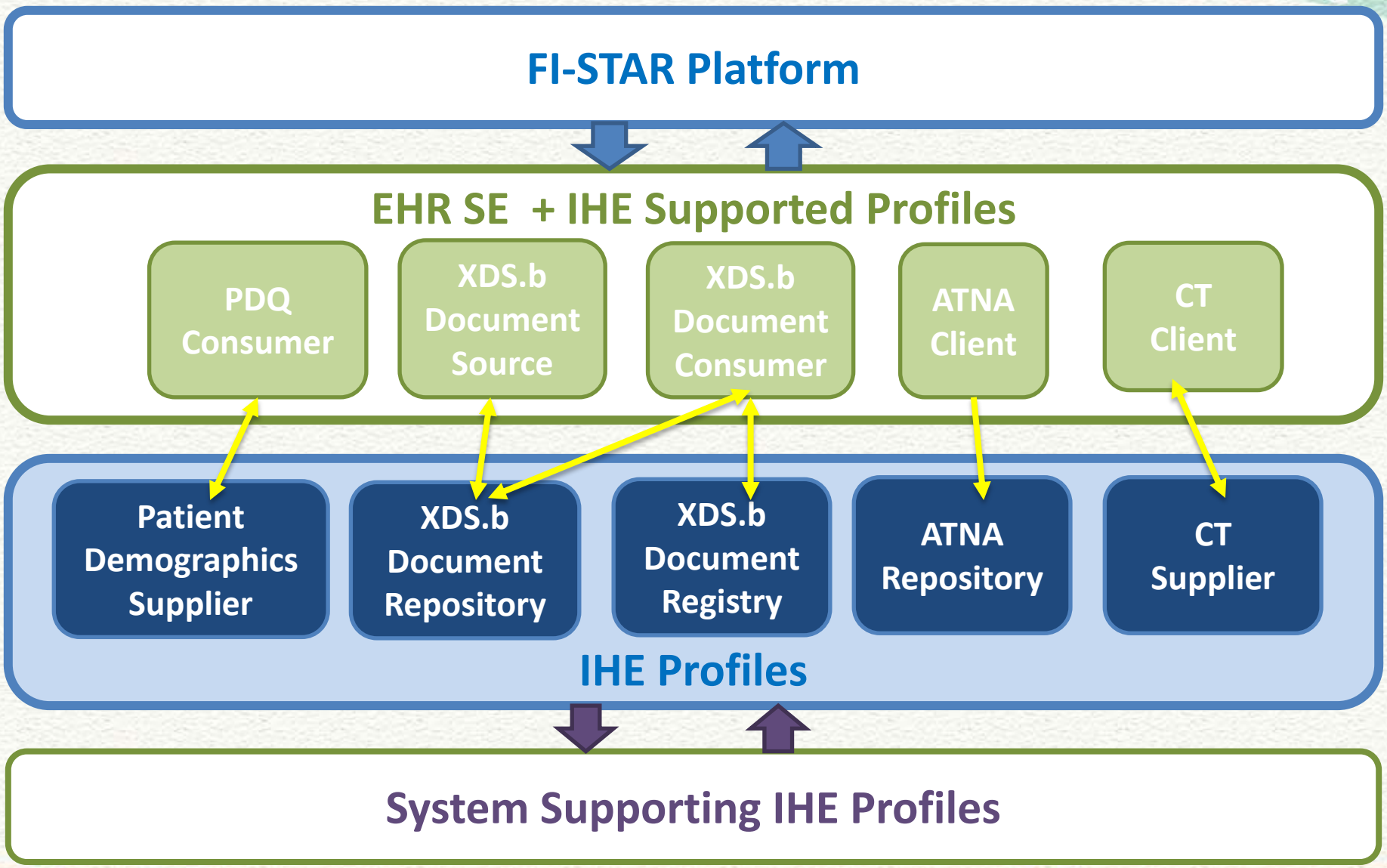
IHE Connectathon provides a unique opportunity for vendors to test the interoperability of their products in a structured environment with peer vendors.

Participants test against multiple vendors using real world clinical scenarios following IHE Integration Profiles specifications

EHR SE supported profiles

Integration Profile	Actor	Results
Audit Trail and Node Authentication	Secure Node	Pass
Consistent Time	Time Client	Pass
Patient Demographic Query HL7 V3	Patient Demographics Consumer	Pass
Cross-Enterprise Document Sharing	Document Consumer	Pass
Cross-Enterprise Document Sharing	Document Source	Pass

EHR SE interoperability benefits



Conclusions

- The problems concerning data protection and privacy for the citizen have been addressed and technological solutions have been developed (I Know).
- Legal issues have been addressed and resolved (they tell me).
- Awareness, training, education are being addressed (I know).
- *eHealth for all* is moving on one-way street (EU knows and takes care of).

XIV MEDITERRANEAN CONFERENCE ON MEDICAL AND BIOLOGICAL ENGINEERING AND COMPUTING

Systems Medicine for the Delivery of Better Healthcare Services

MEDICON 2016

| March 31st – April 2nd, 2016 |

Paphos, Cyprus

Slates from ancient Idalion. Cabinet des Medailles, Paris

Clay hot bottles in the Pafos Museum.

Scalpels with brass handle and iron blade. Found in a surgeon's tomb, in Paphos. Now reside in the Paphos Museum.

Stirrups with brass handle and iron ends. Found in a surgeon's tomb, in Paphos. Now reside in the Paphos Museum.

Iron scissors. Found in a surgeon's tomb, in Paphos. Now reside in the Paphos Museum.

Hot bottle for chest and abdomen. Resides in the Paphos Museum.

Clay hot bottle elbow warmers. Now reside in the Paphos Museum.

Cylindrical copper cases for medicine. Found in a surgeon's tomb. Now reside in the Paphos Museum.

Male genital area clay warmers. Now reside in the Paphos Museum.

Clay hot bottle ear warmers. Now reside in the Paphos Museum.

THANK YOU

eHealth week 11 - 13 MAY 2015 RIGA, LATVIA

ORGANISED BY

Christos N. Schizas
Professor of Computer Science
University of Cyprus
schizas@ucy.ac.cy

Follow us @eHealthWeekEU #eHW15