Prospects for Cloud Computing in a Public University Hospital

Arturo González-Ferrer, Ph.D.

San Carlos University Hospital

Madrid, Spain

Wien, Austria November 23rd 2016

Agenda

1. **Context**
   - **Hospital**
   - **Innovation Unit**
2. **Health IT Security & Cloud**
3. **Our case**
   - **Hospital status**
   - **Regional status**
4. **Prospects: ongoing projects**
5. **Challenges**
6. **Benefits**
7. **Conclusions**

Hospital Clínico San Carlos (HCSC)

- Located in Madrid city center
- Belongs to SERMAS (+30 hospitals)
- 964 beds
- Potentially providing care to 365.000 patients from 14 primary care facilities
- 40.000 admissions, 650.000 outpatient consultations
- 125.000 emergency consultations (350/day)
- More than 5.000 professionals.
  - 807 staff physicians, 453 residents

Hospital Clínico San Carlos
SaludMadrid
Comunidad de Madrid

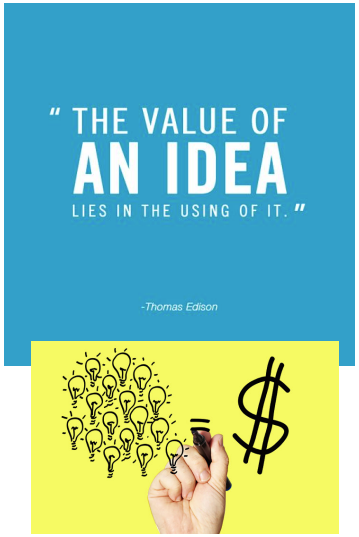
Innovation Unit HCSC

- Main mantra is **to produce VALUE**

- Channeling innovation requests from
  - Hospital professionals
  - External partners
  - Or… proactive proposals by ourselves

- Two main areas:

Develop prototypes of innovative IT, together with external partners	Support the innovation process to move clinical research to market



HealthIT security problems: governance

- Head Directors of IT Department in “Castilla y León” Regional Healthcare System forced to resign this month due to the lost of thousands of medical images during migration of an old IT system

- External company had the **governance** of data and the contract expired…

Un fallo informático provoca la pérdida de miles de radiografías y ecografías

Miles de abulenses deberán repetir radiografías, ecografías y resonancias de las que dependen operaciones y tratamientos oncológicos. Un material obsoleto y la rescisión del contrato con la empresa encargada de mantener el sistema han causado el desastre. Las administraciones guardan silencio, mientras engordan las listas de espera quirúrgicas en la región

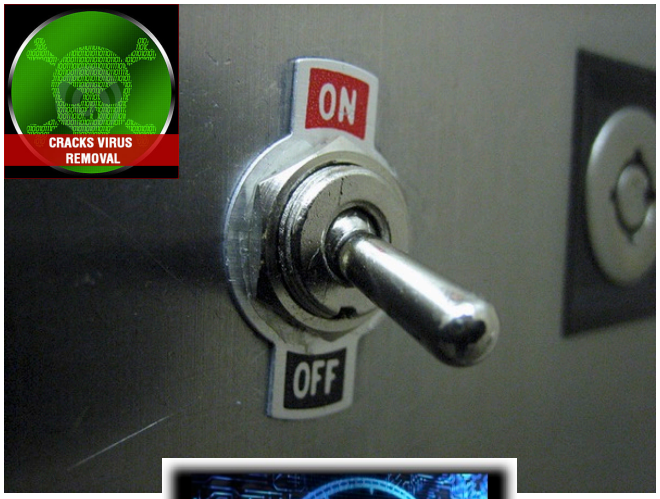
CARLOS LOSPITAO
18/01/2016 | 21:38 H.

Seguir a @CarlosLospitao

ERROR SISTEMA INFORMÁTICO ARCAICO PIERDE

Un error en un sistema informático arcaico pierde miles de pruebas radiológicas.

HealthIT security problems: Virus vs HA



Data Error, Improper PHI Disposal Cause Security Concerns

HIPAA Minimum Necessary Standard Discussed in Hearing

UK hospital system reports computer virus, cancels procedures

The National Health Service's Lincolnshire and Goole trust reported on November 2, 2016 that a computer virus had infiltrated their system, forcing it to cancel "all planned operations, outpatient appointments and diagnostic procedures."

The hospital system said in a statement on its website homepage that the virus infected the computer system on October 30, according to a report on **KrebsonSecurity**.

"We have taken the decision, following expert advise, to shut down the majority of our systems so we can isolate and destroy it," NHS said. "All planned operations, outpatient appointments and diagnostic procedures have been cancelled for Wednesday, Nov. 2 with a small number of exceptions."

The hospital system did not specify the kind of virus that was involved in the incident. Major trauma cases, and also high risk women in labor, were diverted to other hospitals.

As of November 3, **the NHS website's updated statement** said that "the majority of our electronic systems are now back up and working." Patients that were due to come in for an appointment, procedure, operation, or scan were encouraged to come in.

HealthIT security problems: external storage

NOTICE OF DATA PRIVACY EVENT

SILVER CREEK FITNESS & PHYSICAL THERAPY PROVIDES NOTICE OF DATA SECURITY INCIDENT

San Jose, California – October 24, 2016 – Silver Creek Fitness & Physical Therapy, Silver Creek Physical Therapy Gilroy, Silver Creek Physical Therapy Sunnyvale, and Silver Creek Physical Therapy Los Gatos (collectively "Silver Creek") today announced a data incident affecting the security of certain patient records. On September 11, 2016, Silver Creek was notified by its billing and software companies that their Amazon "S3" storage account was vulnerable because it was accessible to persons outside their organization, and that a security researcher who works for a software company accessed and downloaded information from the storage account. This storage account contained, among other things, protected health information of certain Silver Creek patients. The billing and software companies immediately took steps to secure the storage account and launched an investigation to determine to what extent sensitive information was accessed or acquired. They determined that the storage account was vulnerable from May, 2016 to September 11, 2016 and that information was accessed and downloaded by the security researcher on or around September 10, 2016. However, there are no indications that any fraud has resulted from this incident.

"We take any threat to the security of information entrusted to us very seriously," said Mr. Jones, Co-founder of Silver Creek Fitness & Physical Therapy. "Once the error was discovered, we worked with the billing and software companies to ensure that access to the storage account was restricted and that proper access credentials are in place." Mr. Jones added, "We apologize for any inconvenience or concern this incident may cause our patients."

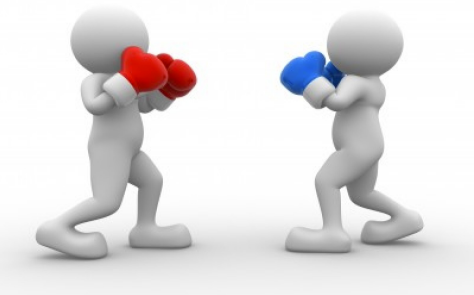
Information Compromised

While Silver Creek Fitness & Physical Therapy, Silver Creek Physical Therapy Gilroy, Silver Creek Physical Therapy Sunnyvale, Silver Creek Physical Therapy Los Gatos has no indications that any fraud has resulted from this incident, it has confirmed that the data affected by this incident possibly includes patient names, Medicare numbers, prescriptions, dates of birth, treatment locations,

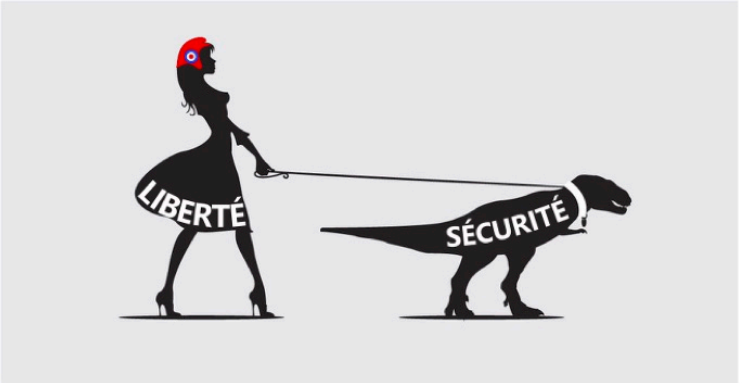
- Patients should have freedom of access to their healthcare data.

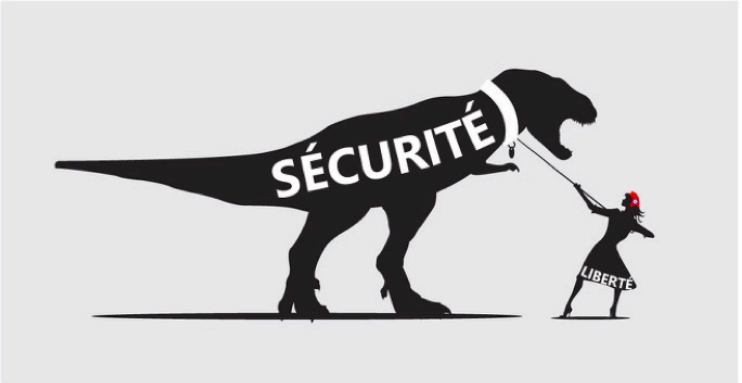
OPEN ACCESS

- Researchers need easy access to patient data.
- Society demands security in this regard
- Security vs Usability? They are usually enemies



who wins?





Review of security in EHRs

- 26/49 used standards or regulations
- 27/49 studies use role-based access control (RBAC)
- 16/49 says emergency justify permission override
- 25/49 audit-log is produced
- **4/49 mention that users, health staff should be trained in security and privacy (!?)**

Journal of Biomedical Informatics 46 (2013) 541–562

Contents lists available at SciVerse ScienceDirect

Journal of Biomedical Informatics

journal homepage: www.elsevier.com/locate/yjbin

Methodological Review

Security and privacy in electronic health records: A systematic literature review

José Luis Fernández-Alemán, Inmaculada Carrión Señor *, Pedro Ángel Oliver Lozoya, Ambrosio Toval

Department de Informatics and Systems, Faculty of Computer Science, University of Murcia, 30100 Murcia, Spain

ARTICLE INFO

Article history:
Received 1 February 2012
Accepted 16 December 2012
Available online 8 January 2013

Keywords:
Electronic health records
Systematic review
Privacy
Confidentiality
Security
Standards

ABSTRACT

Objective: To report the results of a systematic literature review concerning the security and privacy of electronic health record (EHR) systems.
Data sources: Original articles written in English found in MEDLINE, ACM Digital Library, Wiley InterScience, IEEE Digital Library, Science@Direct, MetaPress, ERIC, CINAHL and Trip Database.
Study selection: Only those articles dealing with the security and privacy of EHR systems.
Data extraction: The extraction of 775 articles using a predefined search string, the outcome of which was reviewed by three authors and checked by a fourth.
Results: A total of 49 articles were selected, of which 26 used standards or regulations related to the privacy and security of EHR data. The most widely used regulations are the Health Insurance Portability and Accountability Act (HIPAA) and the European Data Protection Directive 95/46/EC. We found 23 articles that used symmetric key and/or asymmetric key schemes and 13 articles that employed the pseudo anonymity technique in EHR systems. A total of 11 articles propose the use of a digital signature scheme based on PKI (Public Key Infrastructure) and 13 articles propose a login/password (seven of them combined with a digital certificate or PIN) for authentication. The preferred access control model appears to be Role-Based Access Control (RBAC), since it is used in 27 studies. Ten of these studies discuss who should define the EHR systems' roles. Eleven studies discuss who should provide access to EHR data: patients or health entities. Sixteen of the articles reviewed indicate that it is necessary to override defined access policies in the case of an emergency. In 25 articles an audit-log of the system is produced. Only four studies mention that system users and/or health staff should be trained in security and privacy.
Conclusions: Recent years have witnessed the design of standards and the promulgation of directives concerning security and privacy in EHR systems. However, more work should be done to adopt these regulations and to deploy secure EHR systems.

© 2013 Elsevier Inc. All rights reserved.

Data Protection Regulation

Security measures are regulated in sections 89 to 104 of Spanish “Ley Orgánica de Protección de Datos” (Real Decreto 1720/2007) :

	Security measures	Basic Level	Medium Level	High Level
1	Staff Functions and obligations	Si	Si	Si
2	Incident Log	Si	Si	Si
3	Access control	Si	Si	Si
4	Handling of storage and documents	Si	Si	Si
5	Authentication and Authorization	Si	Si	Si
6	Back-up and restore	Si	Si	Si
7	Security responsible		Si	Si
8	Audit		Si	Si
9	Handing of storage and documents		Si	Si
10	Authentication and Authorization		Si	Si
11	Physical access control		Si	Si
12	Incident Log		Si	Si
13	Handling and distribution of storage			Si
14	Back-up and restore			Si
15	Access log			Si
16	Telecommunications			Si

SERMAS

Athene@ Plan: Cloud Center of Regional Health IT Systems (2013)

- Three-DataCenter topology (Active-Active / Contingency)
- Private Cloud for all Madrid health centers
- Consolidation: Virtualization + Standardization
  - Less cost
  - Higher Flexibility, Availability and **Security**

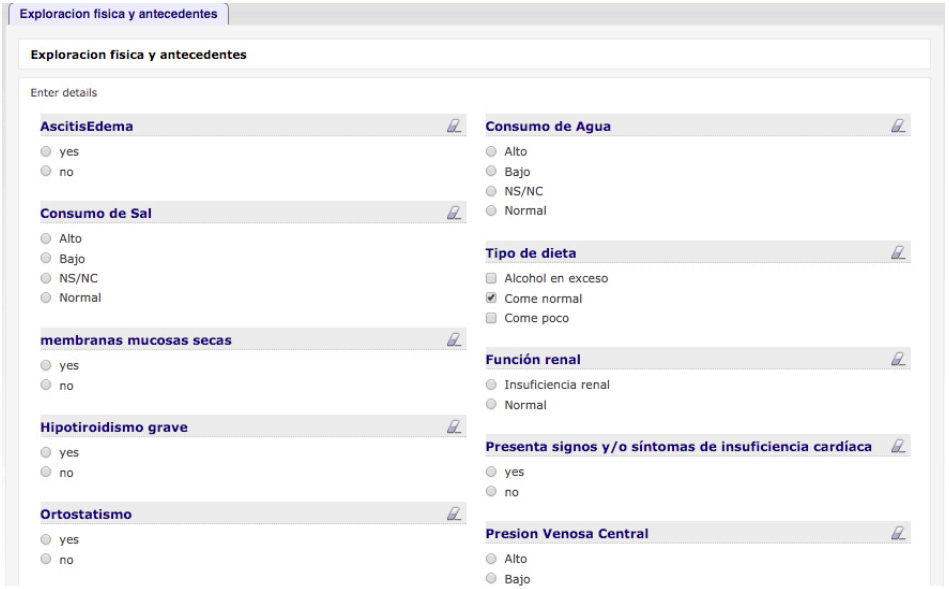
In our institution?

- Many “Data Islands” (lab, pharma, nursing emergency, radiology…)
- 40% of hospital software are self-developments
  - Very difficult to tackle migrations
- No structured EHR (yet)
- Intranet Web application “PACIENTE” (2005) to save discharge patient reports + integration with lab results
- Paper patient medical histories are stored in-hospital but also outside, through a company that **keep, order and transport** them
- No formal CISO (in process)

IaaS or SaaS

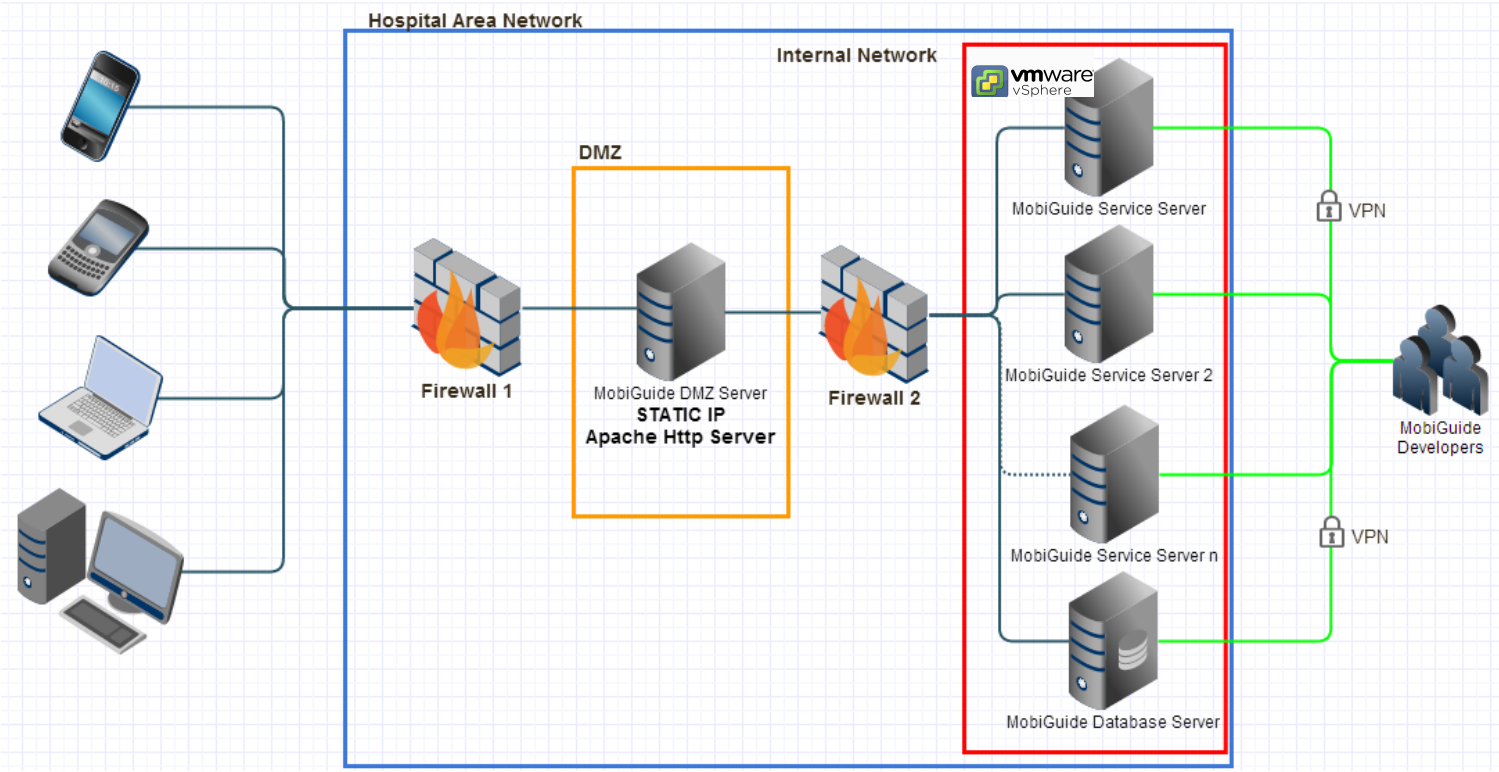
Example: Clinical Decision Support on Hyponatremia

- A web app to collect patient info and get evidence-based decisions



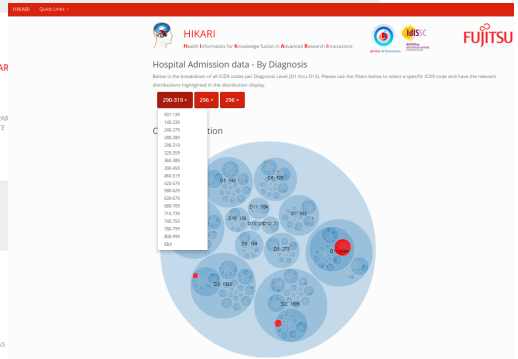
IaaS secure deployment

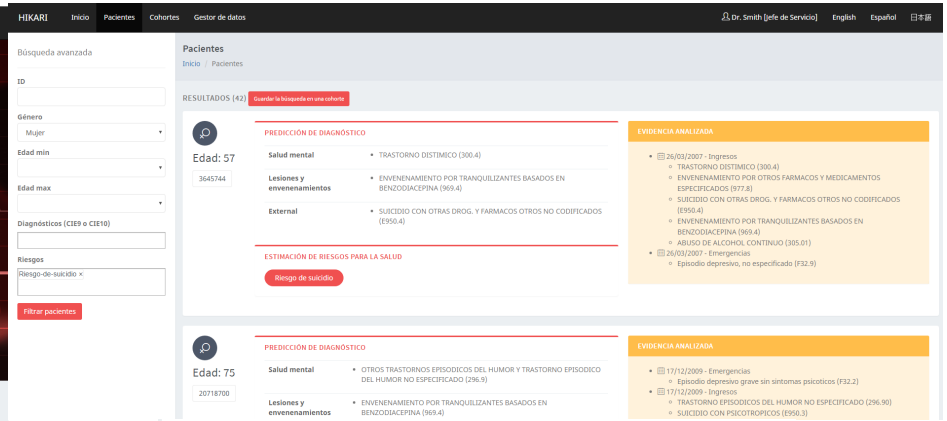
Example: MobiGuide

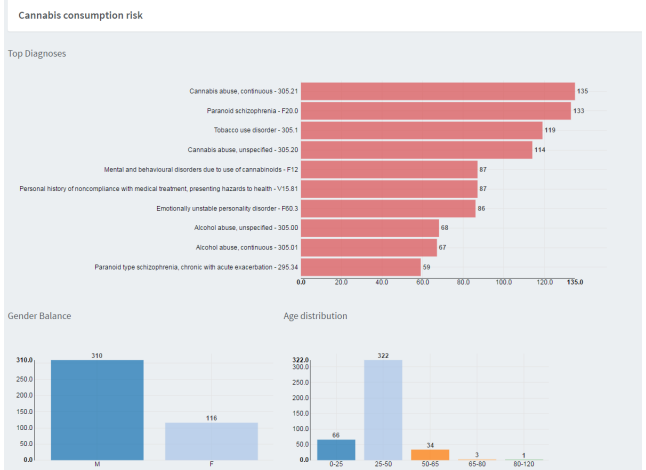


Credits to Daniele Segagni (FSM)

Big Data: HIKARI Project



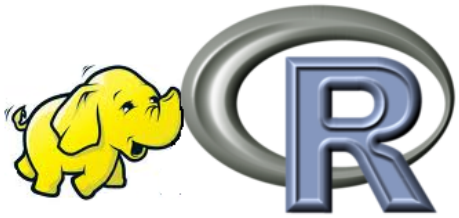


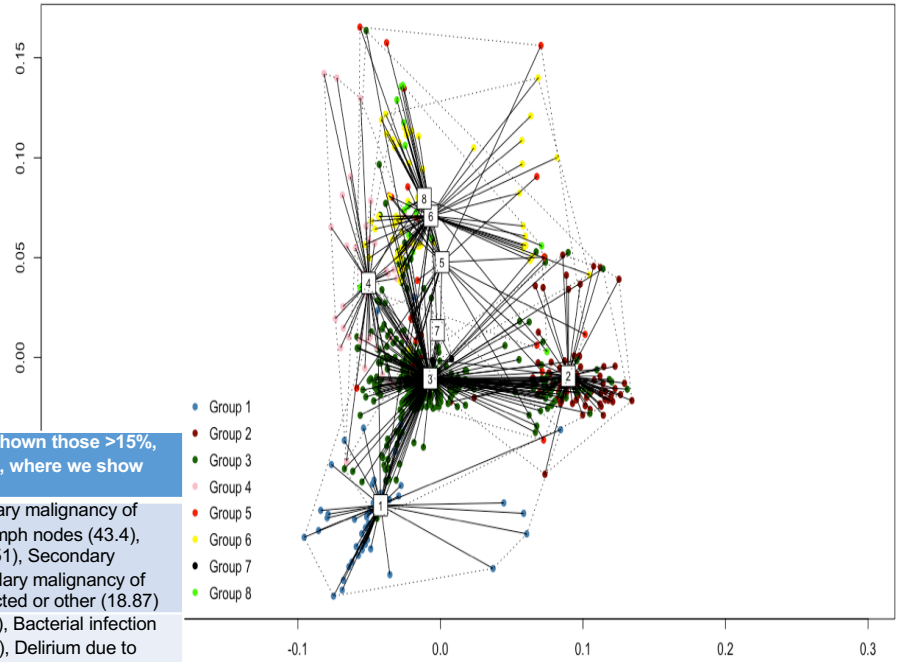


MLaaS: Machine Learning as a Service

- IaaS, SaaS created for Data analytics for healthcare research
- R on Hadoop?

Data outside the Hospital?





Label	Num. Patients	Intra-cluster contribution of variables (shown those >15%, except when not reaching the threshold, where we show those >9%)
Cancer	53	Cancer of bronchus; lung (81.13), Secondary malignancy of bone (45.28), Secondary malignancy of lymph nodes (43.4), Secondary malignancy of brain/spine (41.51), Secondary malignant neoplasm of liver (28.3), Secondary malignancy of respiratory organs (22.64), Cancer, suspected or other (18.87)
UTI	81	Urinary tract infection (95.06), E. coli (32.1), Bacterial infection NOS (29.63), Diaphragmatic hernia (23.46), Delirium due to conditions classified elsewhere (17.28)
NotSpec	351	Urinary tract infection (13.68), Other diseases of respiratory system, NEC (12.54), Encounter for long-term (current) use of aspirin (10.83) Hyperplasia of prostate (9.4)

Easy challenges

- Demonstrate capabilities of the cloud solution for **worst-case scenarios**
  - vulnerabilities in data transfer interfaces
  - breach of data confidentiality
  - breach of data integrity
  - accidental loss of data availability or confidentiality
- Demonstrate **features**
  - Increased protection of personal data
  - provenance and traceability
  - simplicity (e-certificates, vpn's, etc… are not easy for users)

Hard challenges

- **Procurement** can take an age. Each spend must be fully justified, cause serious delays in innovation
- **Institutional and government support.** In our hierarchical structure, is needed.
- **Change & priority management**: You know what *could* be done! But physicians are caring for patients.
- **Patient Sensitive data**: in-house private cloud is costly, outside public cloud is insecure…
- **Cloud providers** cannot see patient data

Benefits

- **Security** is improved, if well implemented
- **Speed-up on backing up** from IT disasters
- **Testing new technologies** can be very fast and independent thanks to virtualization
- **On-demand scalability** for EHR use and research tasks

Conclusions

- **The need for training hospital staff at all levels** prevent doing fast innovations that have impact on their daily activity
- **Security** can be improved over traditional paper-based records. Need to define governance and define usable and hard security policies.
- **Actual benefit**: reduction of costs and backup. **Prospect**: MlaaS, CDSS,…
- **Using virtualization,** care professionals can explore new IT solutions
- To reach hospitals, success rely on iterative approach: cheap scenario-based prototypes that work can end up on **value-based investments**

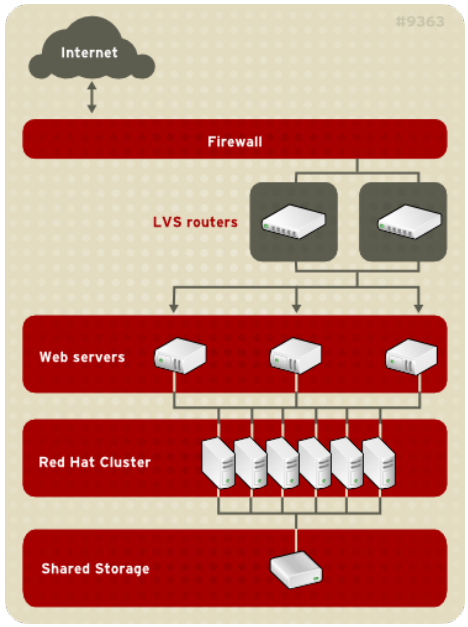
”You are now inside the mirror dimension, ever present but undetected. The real world isn't affected by what happens here. We use the mirror dimension to train, surveil and sometimes to contain threats”.

Thank you

Dr. Strange (2016)

Cloud: a parallel dimension that allows the user to practice their magical abilities ~~without the public's knowledge~~

About myself: arturogf@gmail.com

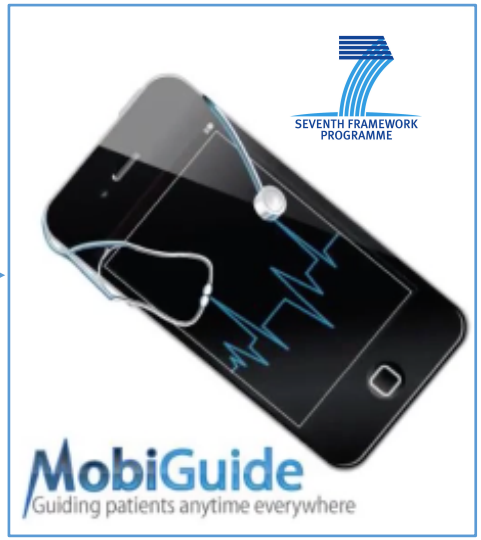


Universidad de Granada

2002

Designed the e-learning service. 30.000 students. HA with GFS2 + SAML2-Shibboleth federated Auth.

Ph.D.



אוניברסיטת חיפה
UNIVERSITY OF HAIFA

2010

Leaded the Data Integration Tasks within a 5M€ EU-funded FP7 project to develop a patient guidance system

UC3M University

2013

Healthcare Data Analytics

Unidad de Innovación

IdISSC
INSTITUTO de INVESTIGACIÓN SANITARIA
Hospital Clínico San Carlos

Process Support and Knowledge Representation in Health Care

Hospital Clínico San Carlos
SaludMadrid
Comunidad de Madrid

2015

supports the institution taking IT innovations that can provide some value for improvement

Today