Proposing

A Secure and Distributed Infrastructure for Health Record Access

Victoriano Giralt

Central ICT Services
University of Málaga

IARIA ICDS 2012
Ciudad Politécnica de la Innovación
Valencia
February 1st, 2012

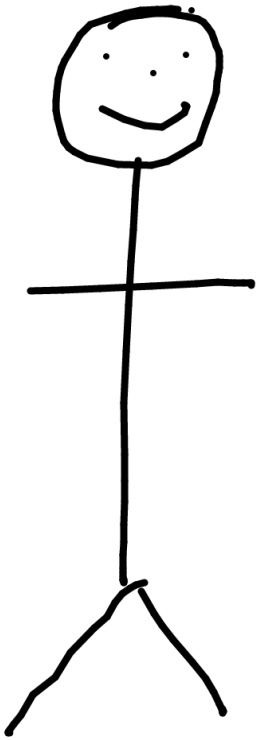
Introducing some characters

SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

Patient

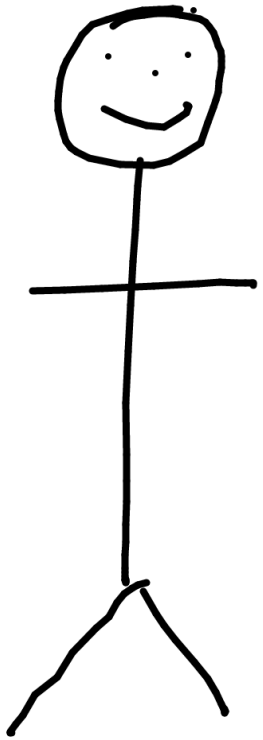
a.k.a. *you or me*



Hi! I'm the patient

Patient

a.k.a. *you or me*



i.e. *you*

Practitioner

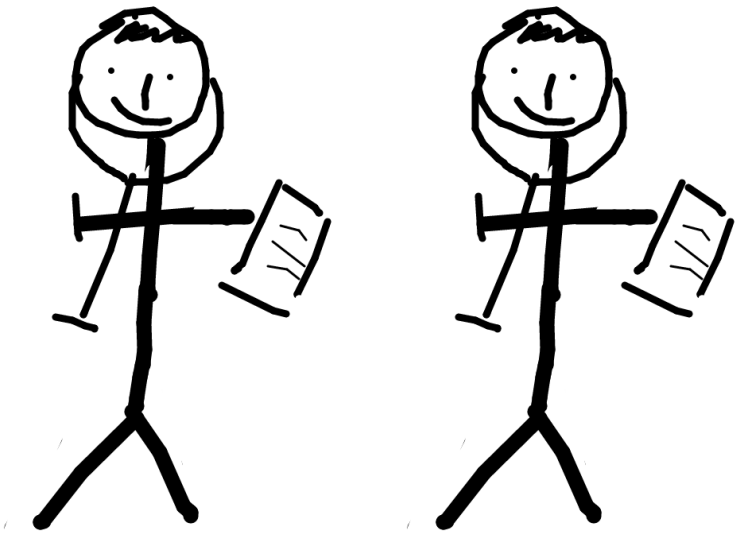
a.k.a. *The* Doctor

Hi! I'm your doctor

SSEDIC Programme Partner

Practitioner

a.k.a. *The* Doctor



Hi! I'm also your doctor

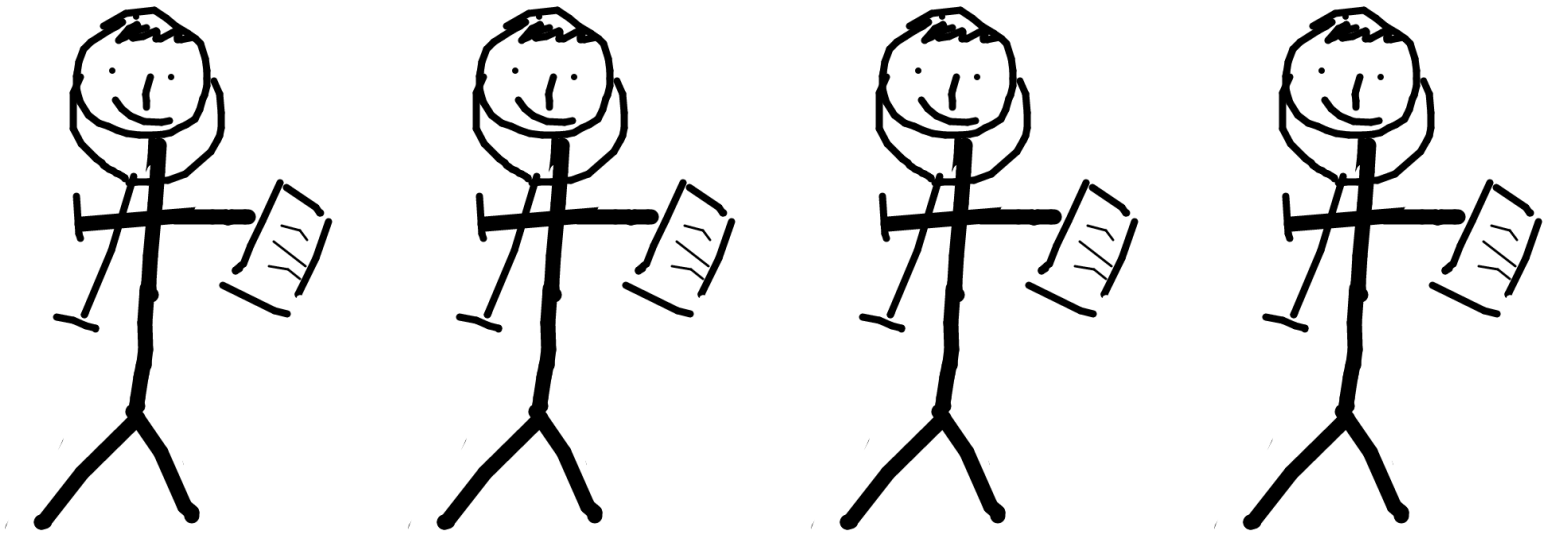
Practitioner

a.k.a. *The* Doctor

Me too!

Practitioner

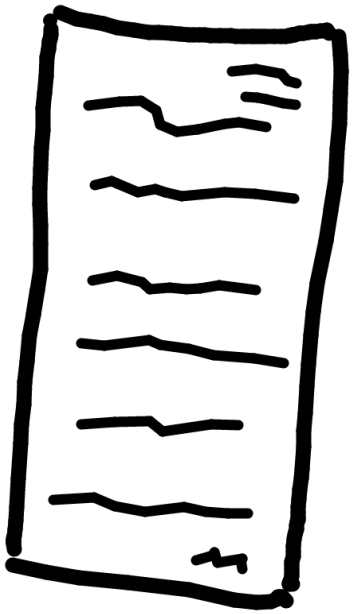
a.k.a. *The* Doctor



we all are your doctors

Health Record

a.k.a. *lots of data about me*

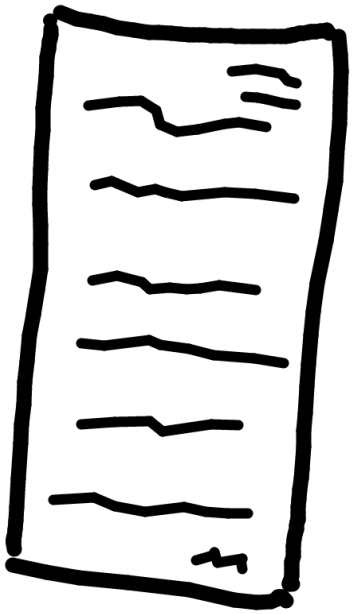


Hi! I'm your Health Record

SSEDIC Programme Partner

Health Record

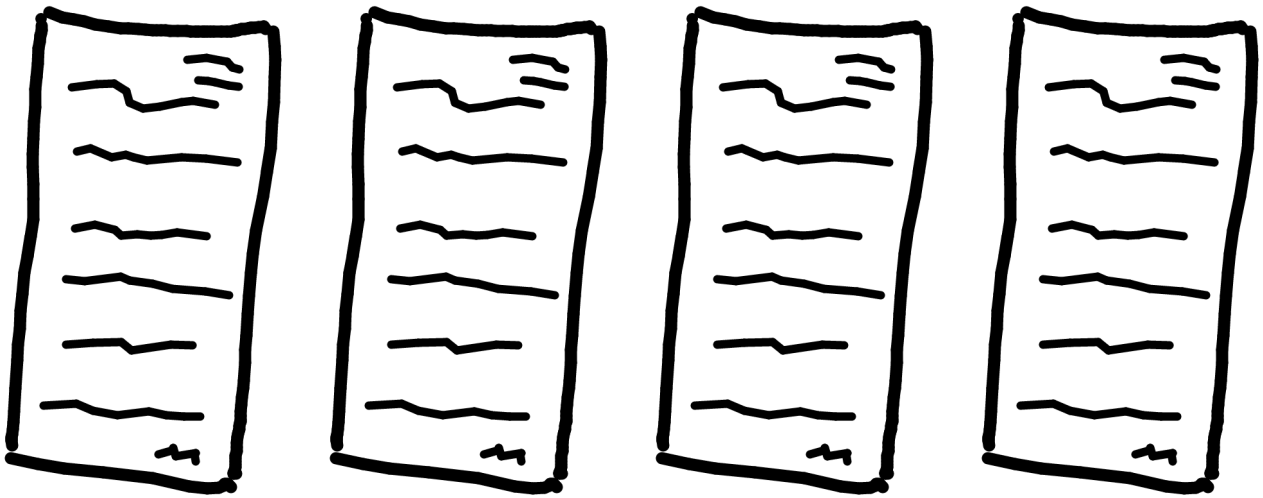
a.k.a. *lots of data about me*



Only me?

Health Record

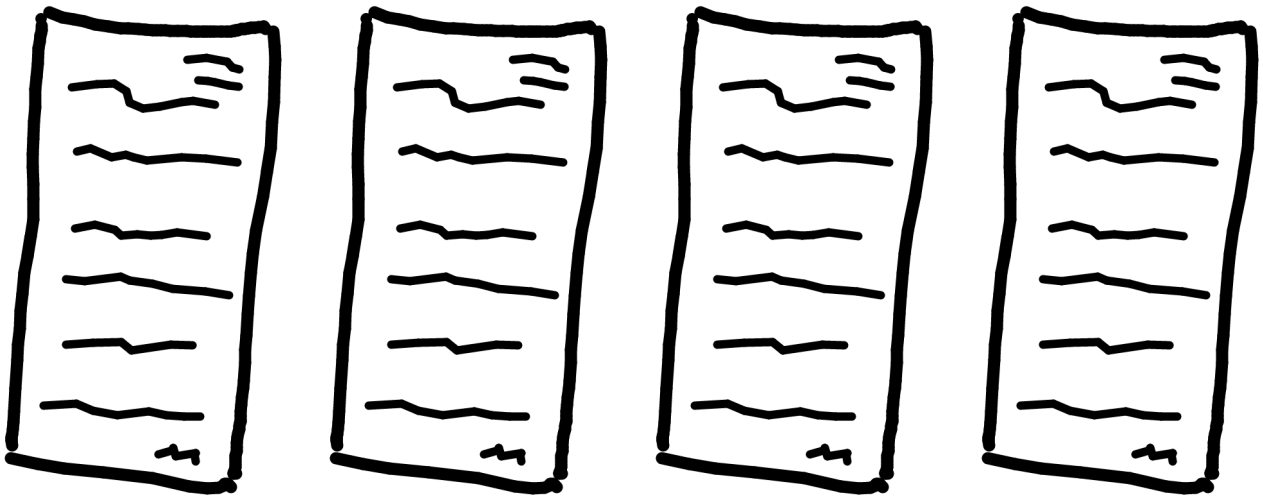
a.k.a. *lots of data about me*



Or us?

Health Record

a.k.a. *lots of data about me*

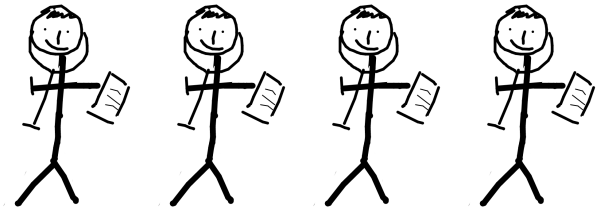


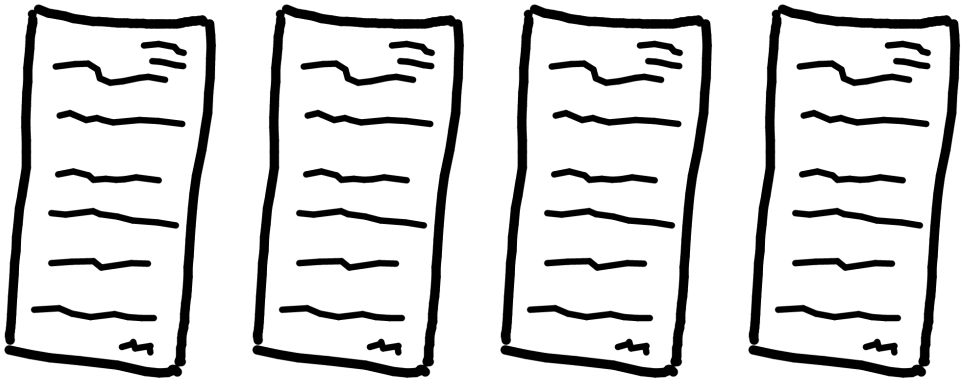
Really yours?

SSEDIC Programme Partner

Health Record

a.k.a. *lots of data about me*

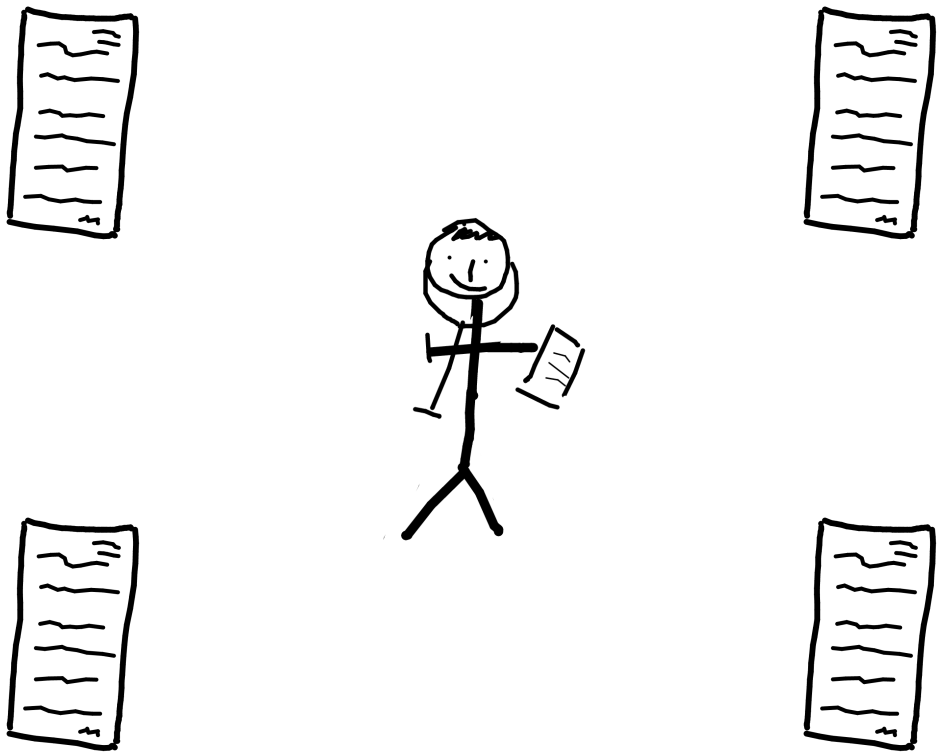




Or theirs?

Present situation

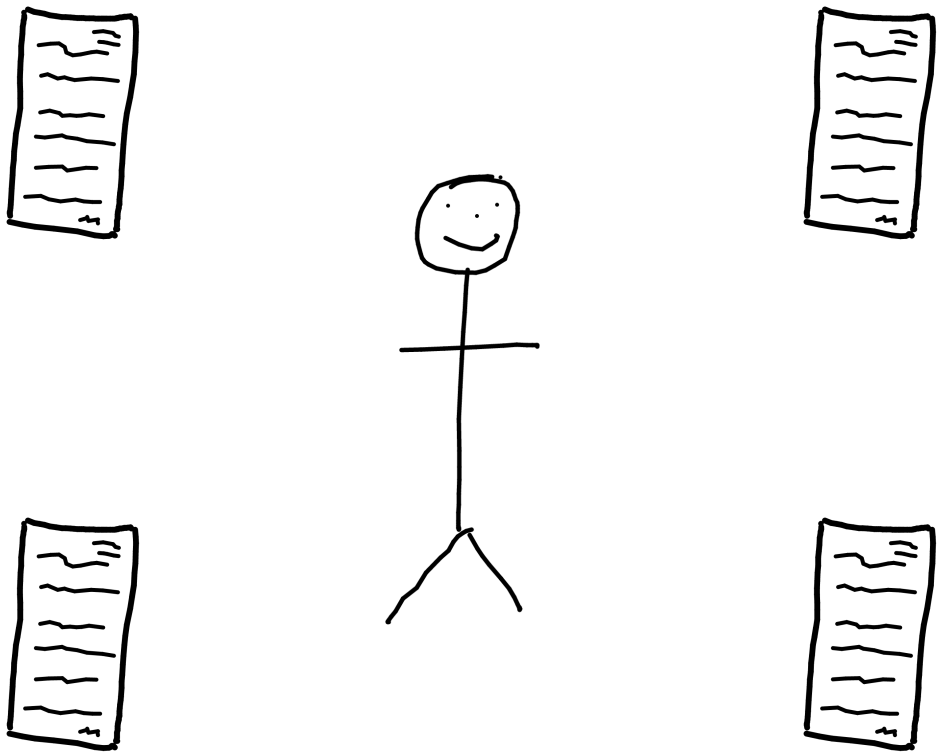
someone controls *my* data



Someone owns *my* HRs

Proposed situation

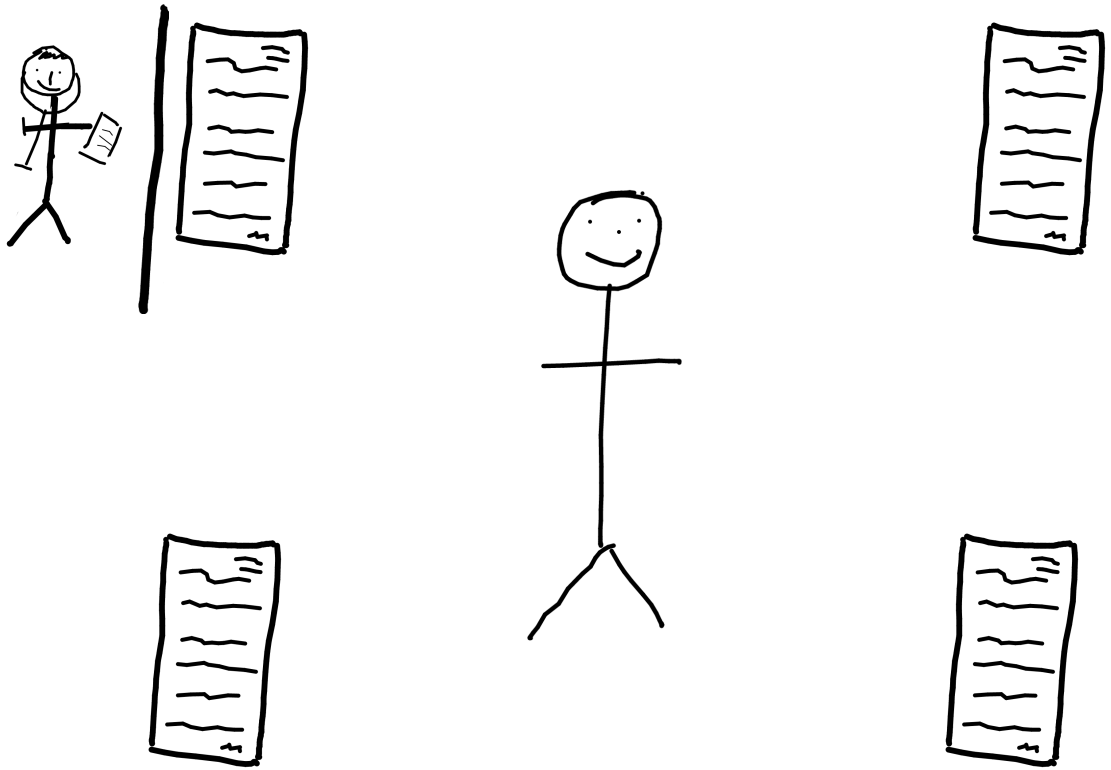
I control *my* data



I own my Heatlh Records

Proposed situation

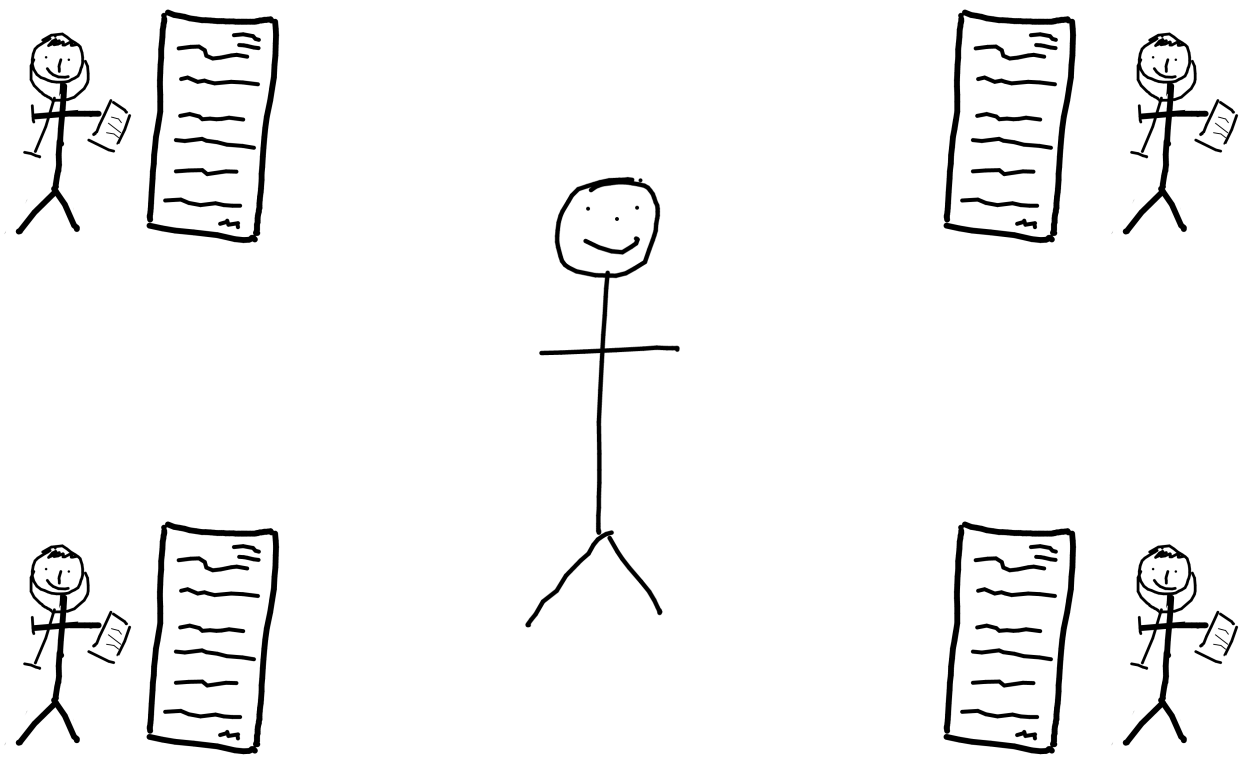
I control *my* data



I *control* access to my HRs

Proposed situation

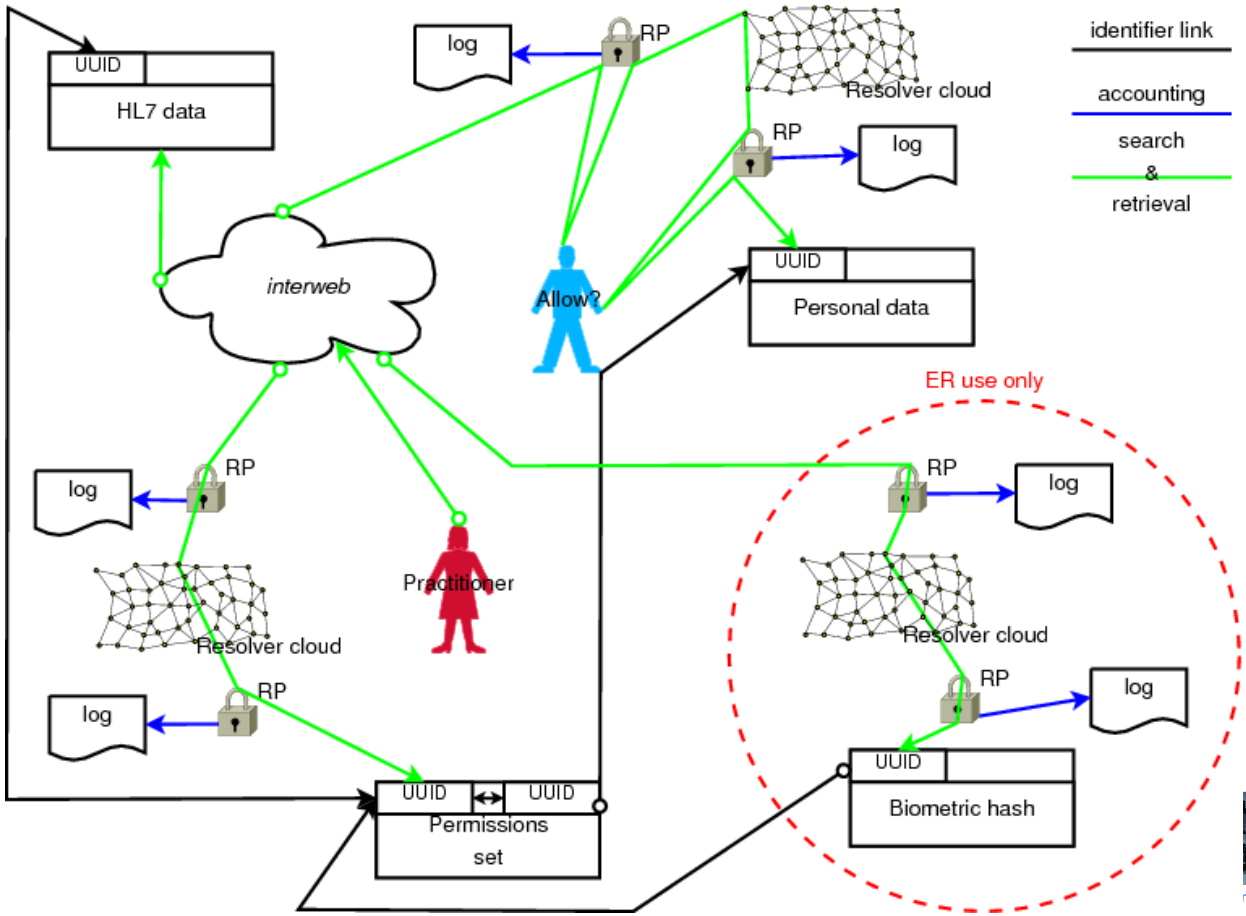
I control *my* data



I *know* **who** is using my HRs

System map

a.k.a. the big picture



User stories

explaining the big picture

1. Individual enrolment
2. Creation of health record in clinical practice
3. Access to health records in clinical practice
4. Access to health records from the emergency room
5. Access to health information for research purposes
6. Access to personal identity information

SSEDIC Programme Partner

Technical terminology

Electronic identity terms

SSEDIC Programme Partner

Technical terminology

Electronic identity terms

- Individual

Identifiable Individual

A single physical person than can be identified by a set of personal data that constitutes their identity record.

Technical terminology

Electronic identity terms

- Individual
- Attribute

Attribute

A property of an identity record consisting of one or more values. All the values of an identity attribute are related by a common purpose or meaning.

SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

Technical terminology

Electronic identity terms

- Individual
- Attribute
- Principal

Identity Principal

A person for whom another entity acts as an agent or representative.

Technical terminology

Electronic identity terms

- Individual
- Attribute
- Principal
- Pseudonym

Pseudonymous identifier

An identifier that can single out an individual without revealing the real identity.

Technical terminology

Electronic identity terms

- Individual
- Attribute
- Principal
- Pseudonym
- Biometric

Biometric information

Personal information attributes derived from physical or biological characteristics of an individual.

Technical terminology

General information processing and storage terms

SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

Technical terminology

General information processing and storage terms

- Hash

Hash Value

The result of using a hashing function on an element of a data set. These functions transform larger data sets into smaller ones and produce the same result given the same input.

SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

Technical terminology

General information processing and storage terms

- Hash
- UUID

Universally Unique Identifier

A 16 byte (128 bits) string that is guaranteed to be different from all other UUIDs generated before 3603 A.D., if the recommended algorithms are used.

SSEDIC Programme Partner

Technical terminology

General information processing and storage terms

- Hash
- UUID
- Resolver

Resolver

An entity that can link pseudonymous identifiers like UUIDs to information about principals with or without identifying them.

Technical terminology

Federated Identity and Access Management terms

SSEDIC Programme Partner

Technical terminology

Federated Identity and Access Management terms

- IdP

Identity Provider

An entity able to identify individuals and provide attributes pertaining to their identity.

Technical terminology

Federated Identity and Access Management terms

- IdP
- Federation

Identity Federation

Infrastructure supporting the trust links between IdPs and RPs.

Technical terminology

Federated Identity and Access Management terms

- IdP
- Federation
- RP

Relying Party

An entity that trusts the federation and accepts identities asserted by IdPs.

SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

Technical terminology

Federated Identity and Access Management terms

- IdP
- Federation
- RP
- AS

Authorisation Server

A trusted entity that takes access decisions based on attributes of the principals involved in a transaction in support of an RP.

Technical terminology

Federated Identity and Access Management terms

- IdP
- Federation
- RP
- AS
- AA

Attribute Authority

A trusted entity that asserts attributes about principals with or without revealing their identities to other principals involved in a transaction.

SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

Technical terminology

Federated Identity and Access Management terms

- IdP
- Federation
- RP
- AS
- AA
- LoA

Level of Assurance

The level of confidence with which the identity of an individual has been vetted in order to be linked to an electronic identity record.

Technical terminology

Medical terms

SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

Technical terminology

Medical terms

- HL7

Health Level Seven

An international standards organisation that works for the interoperability of health clinical and administrative data. And, it is also used to refer to the standards defined by said organisation.

Technical terminology

Medical terms

- HL7
- Act

Health Care Act

One of the three main classes defined in the HL7 reference information model (RIM) that represent actions that are executed and must be documented as various parties provide health care.

Technical terminology

Medical terms

- HL7
- Act
- Role

Role

Second of the main classes defined in the HL7 RIM that establishes the function played by entities as they participate in health care acts.

SSEDIC Programme Partner

Technical terminology

Medical terms

- HL7
- Act
- Role
- Entity

Entity

Third of the classes that represents the physical things and beings that are of interest to, and take part in, the health care.

SSEDIC Programme Partner

Technical terminology

Medical terms

- HL7
- Act
- Role
- Entity
- Relationship

Act Relationship

Represents the binding of one act to another.

Technical terminology

Medical terms

- HL7
- Act
- Role
- Entity
- Relationship
- Participation

Act Participation

Expresses an act's context, such as who performed it, for whom and where.

SSEDIC Programme Partner

Technical terminology

Medical terms

- HL7
- Act
- Role
- Entity
- Relationship
- Participation
- Link

Role Link

Represents relationships between individual roles.

Technical terminology

Medical terms

- HL7
- Act
- Role
- Entity
- Relationship
- Participation
- Link
- HR

Health Record

A collection of health information related to an act or to the general health state of an individual.

SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

Technical terminology

Protocols and acronyms, a.k.a. letter soup

SSEDIC Programme Partner

Technical terminology

Protocols and acronyms, a.k.a. letter soup

- SAML

Security Assertion Markup Language

XML based protocol for expressing trust via electronic means and asserting information about principals in widespread use in present identity federations.

It allows for inter-domain authentication, authorisation and accounting of access to resources.

SSEDIC Programme Partner

Technical terminology

Protocols and acronyms, a.k.a. letter soup

- SAML
- OAuth

Open Authorisation

A protocol that allows third party access to data with express authorisation of the owner of that data.

Technical terminology

Protocols and acronyms, a.k.a. letter soup

- SAML
- OAuth
- DHT

Distributed Hash Tables

A class of decentralised distributed system that provides a look-up service similar to a hash table. (key, value) pairs are stored in a DHT, and any participating node can efficiently retrieve the value associated with a given key.

SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

Actors

for the user story plays

SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

Actors

for the user story plays

- Patient

Patient

A person that is the subject of a medical act.

SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

Actors

for the user story plays

- Patient
- Practitioner

Practitioner

Any health care professional of any kind that interacts with patients in medical acts.

Actors

for the user story plays

- Patient
- Practitioner
- ERP

Emergency Room Practitioner

A practitioner assigned to an Emergency Room that will have special access in the stories.

SSEDIC Programme Partner

Actors

for the user story plays

- Patient
- Practitioner
- ERP
- Staff

Staff member

Non medical professionals that have a role in medical acts that require access to partial content of the HRs or to personal data of the patients.

Actors

for the user story plays

- Patient
- Practitioner
- ERP
- Staff
- Relative

Patient Relative

A person with a family or other kind of social relationship to a patient that might play a role in authorising access to HR or provide personal information about the patient.

SSEDIC Programme Partner

Actors

for the user story plays

- Patient
- Practitioner
- ERP
- Staff
- Relative
- Researcher

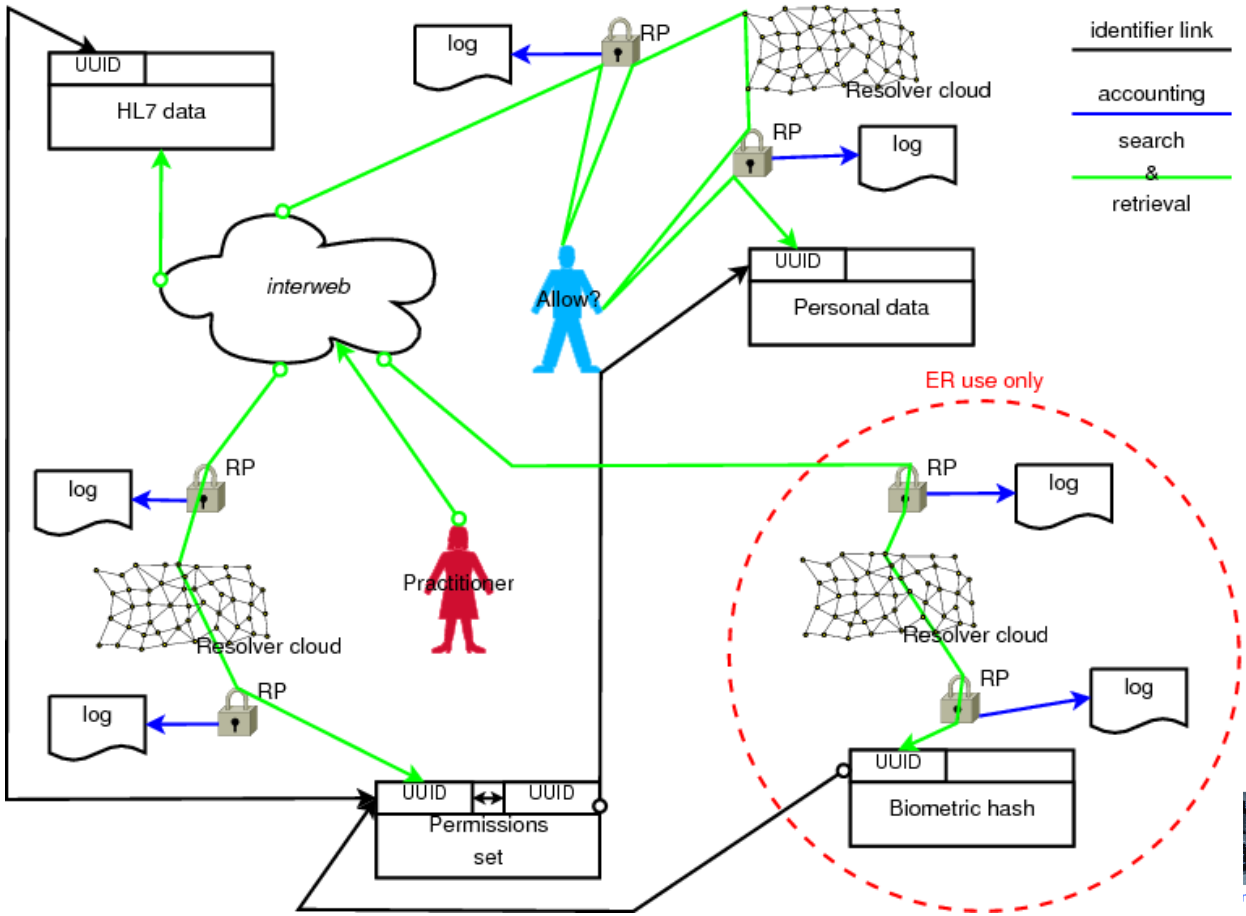
Researcher

A person that requires anonymous, or, at most, pseudonymous access to HRs for scientific research work.

SSEDIC Programme Partner

System map

a.k.a. the big picture, revisited



Individual enrolment

I'm a patient and want to publish my HR

1. I select an IdP or
   the national health system provides me one.
2. I identify to the IdP using documents to
   achieve the required LoA and provide
   contact information for me and my closest relative.
3. I get the UUID that identifies my personal data.
4. My UUID is published by the IdP resolver.
5. My biometric hash is published in the resolver cloud.
6. I get my biometric hash UUID and link it to my UUID.

SSEDIC Programme Partner

Creation of health record in clinical practice

1. I as a patient go visit a practitioner.
2. All acts are compiled into HR documents.
3. The HR are dated and get UUIDs.
4. The HR UUIDs and my UUID are inserted in my IdP resolver.
5. The HR UUIDs the pertinent pointer are sent to the resolver finder cloud from the resolver.

SSEDIC Programme Partner

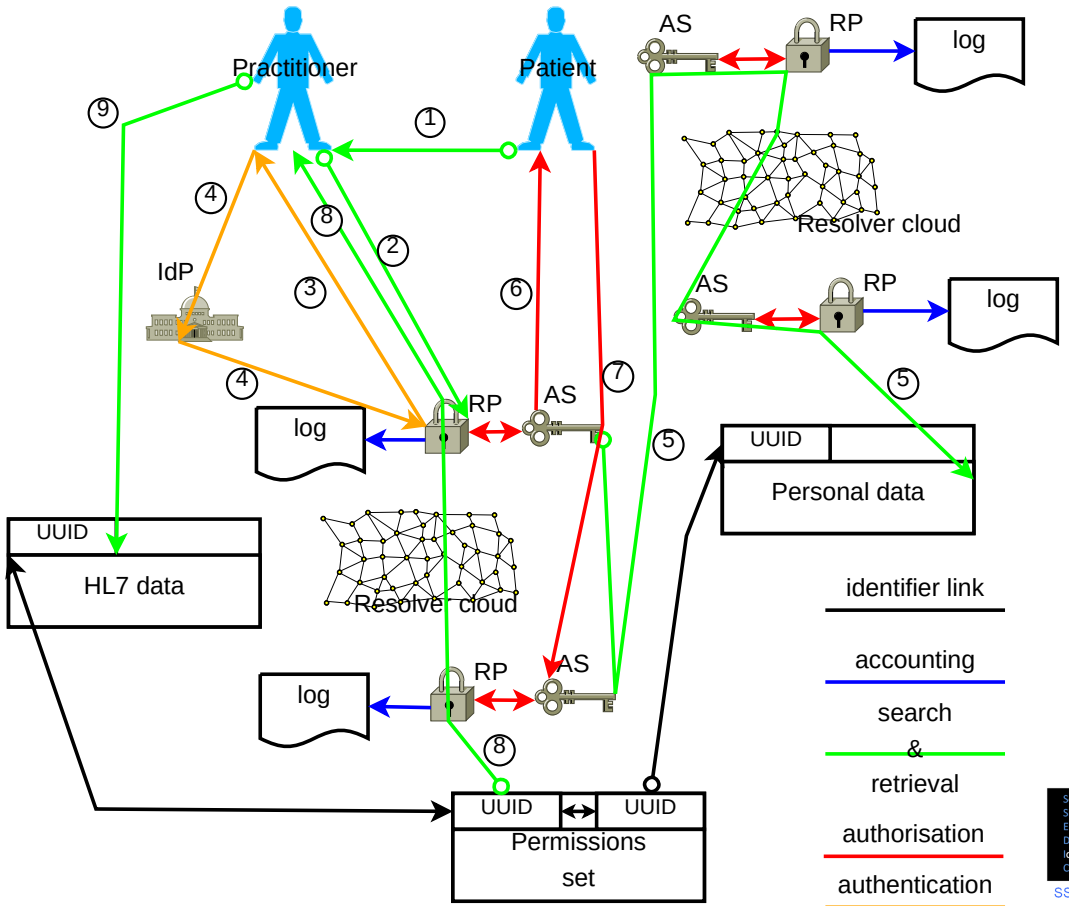
Access to health records in clinical practice

1. I as a patient go visit a practitioner.
2. The practitioner requests historic HR information.
3. I provide the practitioner with my UUID.
4. The practitioner identifies to the pertinent IdP and queries the resolver finder cloud and then, the appropriate resolver.
5. The resolver AS sends me a message indicating the practitioner identity, information about the requested data and a request for granting authorisation.
6. I grant the access and set a time limit.
7. The practitioner can access the data.

SSEDIC Programme Partner

Access to health records in clinical practice

a *smaller* picture



Access to health records from the emergency room

1. An unconscious and unidentified patient arrives in life threatening conditions.
2. Standard biometric parameters are determined and hashed.
3. A practitioner in the ER identifies to an IdP connected to an AA that asserts the attributes that verify the ER role.
4. The asserted attributes allow access to resolvers for biometric hashes.

Access to health records from the emergency room

5. Attributes allow access to UUID resolvers without requesting authorisation from the patient or relatives.
6. The resolvers return all HR UUIDs related to the UUID associated to the biometric hash.
7. The ER practitioner can retrieve the whole history of HRs without any knowledge of the identity of the individual.

Access to health information for research purposes

1. I am a researcher working on a certain disease.
2. I search the web an collect all pertinent HRs.
3. I need to know about historic HR data about the same individuals that form the population under study.
4. I identify to my IdP that has an AA that asserts attributes to prove my researcher condition.
5. I query the resolvers for other HR UUIDs that belong to the same individuals as the HR UUIDs in the collection under study.
6. Depending on user preferences, data sensitivity or other parameters, patients get a request for granting access to the HR.

SSEDIC Programme Partner

Access to personal identity information

1. I am a hospital staff member.
2. I need to know a patient identity for billing purposes.
3. I identify to the hospital IdP and the hospital AA asserts attributes to prove my administration staff status.
4. I query the resolver finder cloud to find the resolver for the patient UUID.
5. I query the patient resolver.
6. I get back the data needed to bill the patient.
7. The patient is notified of the personal data request.

SSEDIC Programme Partner

Future

a lot of pending work

- Build a prototype demonstrator
- Validate functionality
- Present PhD dissertation
- Extend to other domains

SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

Thank you

SSEDIC Programme Partner

UNIVERSIDAD DE MÁLAGA

Thank you

Questions?

answers not assured

SSEDIC Programme Partner