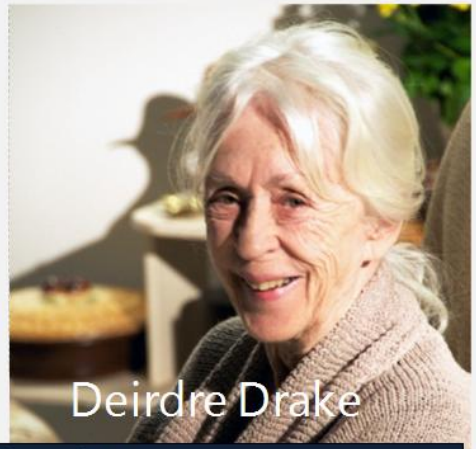
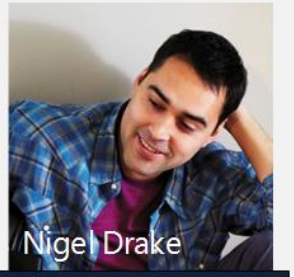
# A Next Generation Cloud-based Health Care Platform

Prof Bill Buchanan, Dr Lu Fan, Prof Christoph Thuemmler, Dr Elias Ekonomou, Owen Lo, and Alistair Lawson, Edinburgh Napier University.

- Healthcare Professional.
- Invited user




- Care Subject
- 82 years old
- House bound
- COPD (Chronic Obstructive Pulmonary Disease)




- Invited user

- GP.
- Invited user

- Site Creator
- Primary Carer

Assisted Living (Informal and Trust based)

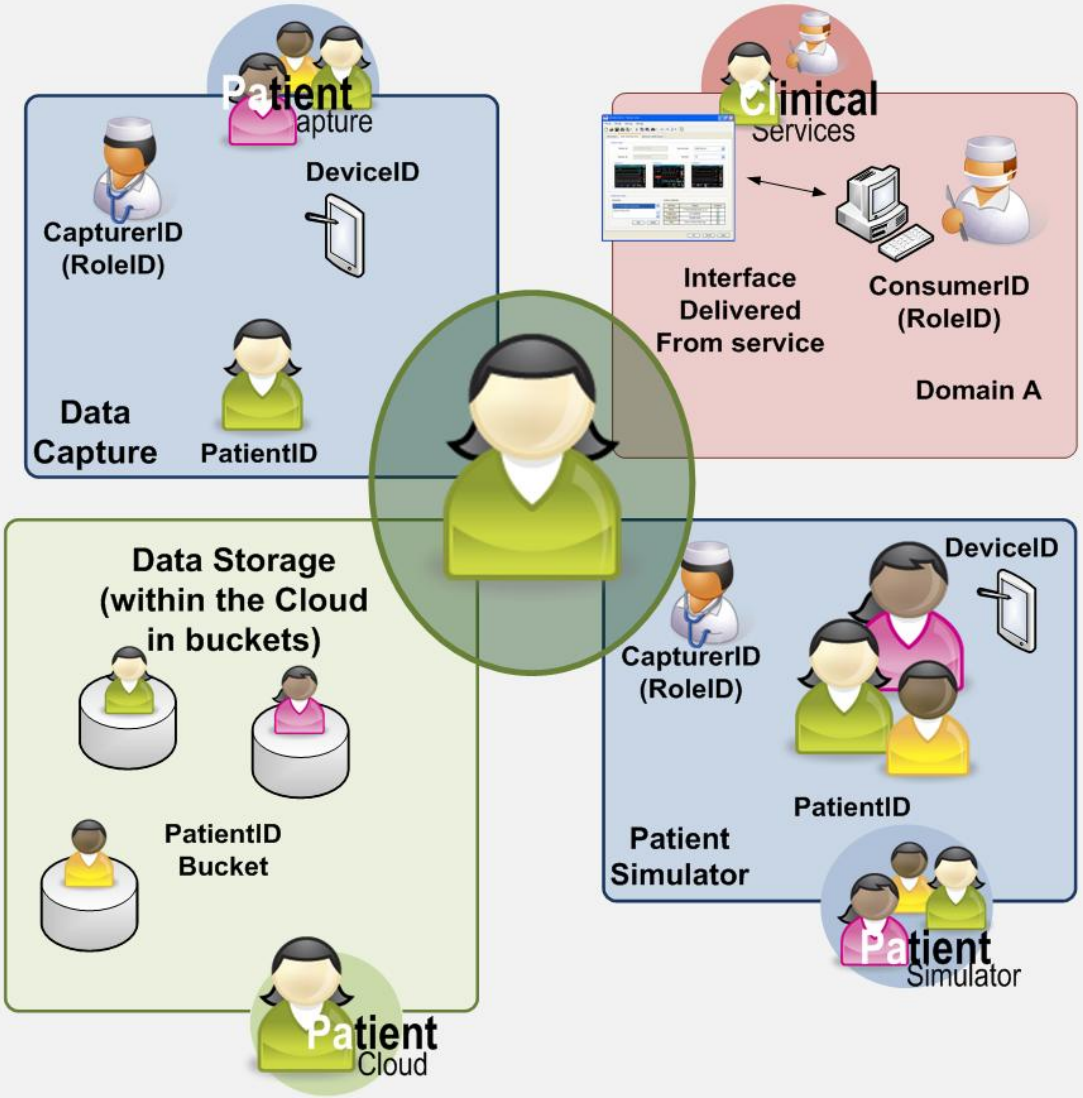
Primary Health Care (Formal and role-oriented) - GP

Secondary Health Care (Formal and role-oriented) - Hospitals/A&E

Social Care/Health/etc

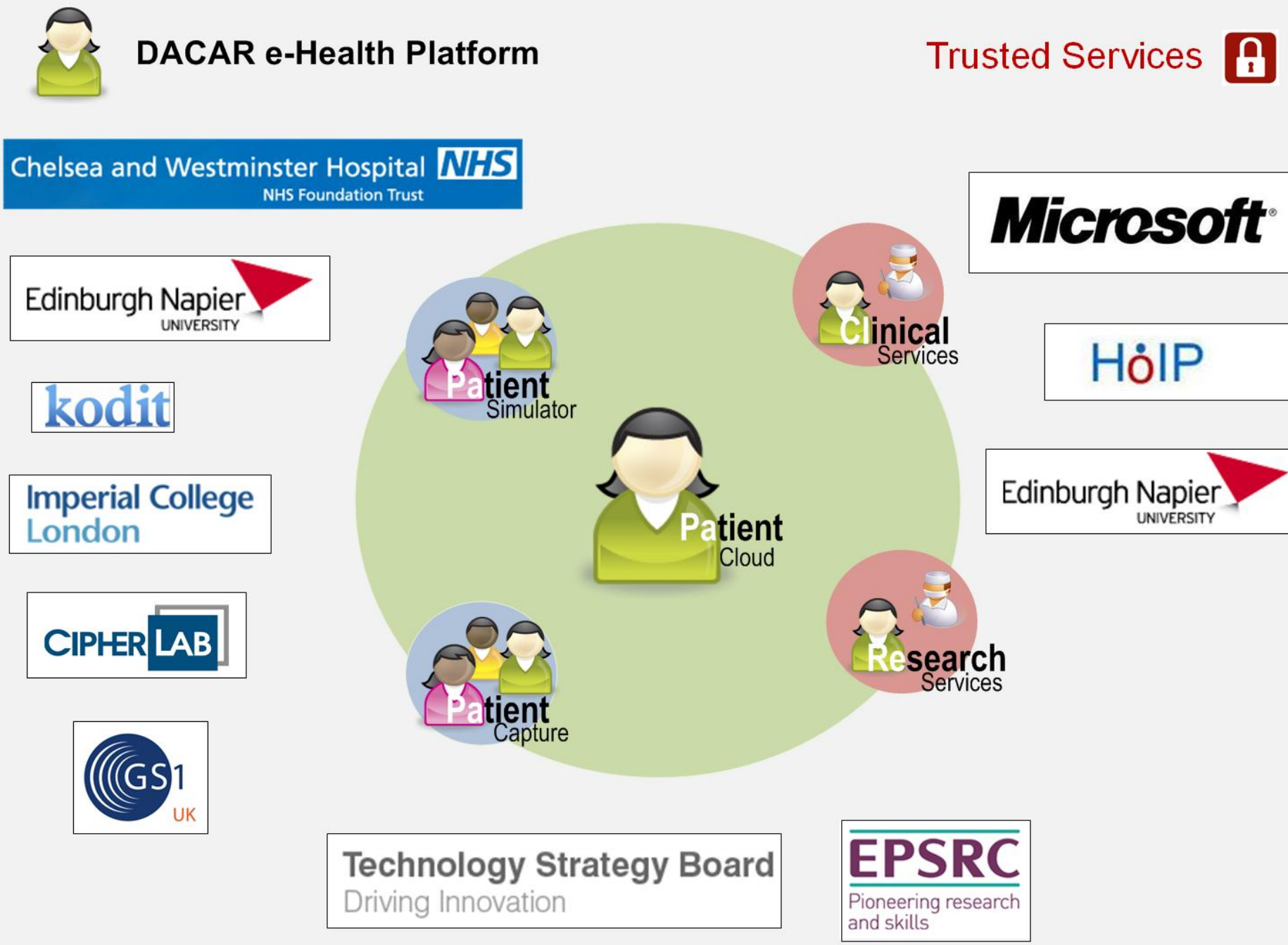
**PatientCloud:**
Funded by EPSRC and TSB, and is a collaboration between C&W, Imperial College, Edinburgh Napier University, Kodit, GS1 and Ciperlab

# Introduction/ Context



# DACAR e-Health Platform

Trusted Services



## Societal

## Technical

Lack of integration between assisted living, primary and secondary care

Patient records are often static

Aging population

Different systems/formatting used for data

Lack of information sharing across the public sector

Limited/difficult access methods … typically Government infrastructures … lack of trust

Strong demand to consume health care data

Poor access control to data

Lack of integration with careers and trusted people

Data often aggregated and context is often lost

Some key issues

**PatientCloud:**
Funded by EPSRC and TSB, and is a collaboration between C&W, Imperial College, Edinburgh Napier University, Kodit, GS1 and Ciperlab

Rights

Clinical Services

Digital Trust

Human Trust

Strong Governance

Identity

Infinite possiblities

Translation of rights
Translation of identities

Strong Governance
Policy

Assisted Living (Informal and Trust based)

Primary Health Care (Formal and role-oriented)

Secondary Health Care (Formal and role-oriented)

**Manager might ask:** What's difference in length-of-stay between different age categories for June?

**Consultant might ask:** How does the Early Warning Score affect the length-of-stay?

**Family friend might ask:** In which ward is Deirdre?

**PatientCloud:**
Funded by EPSRC and TSB, and is a collaboration between C&W, Imperial College, Edinburgh Napier University, Kodit, GS1 and Ciperlab

PatientID

**Static Patient Record**

- Often localised
- Different systems/formats
- Poor access control
- Poor identity verification
- Cannot be aggregated
- Etc.

ConsumerID (RoleID)

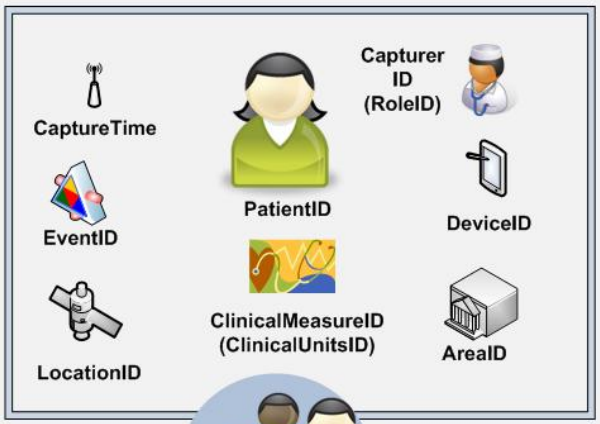
Domain A

**Data Storage (within the Cloud in buckets)**

PatientID Bucket

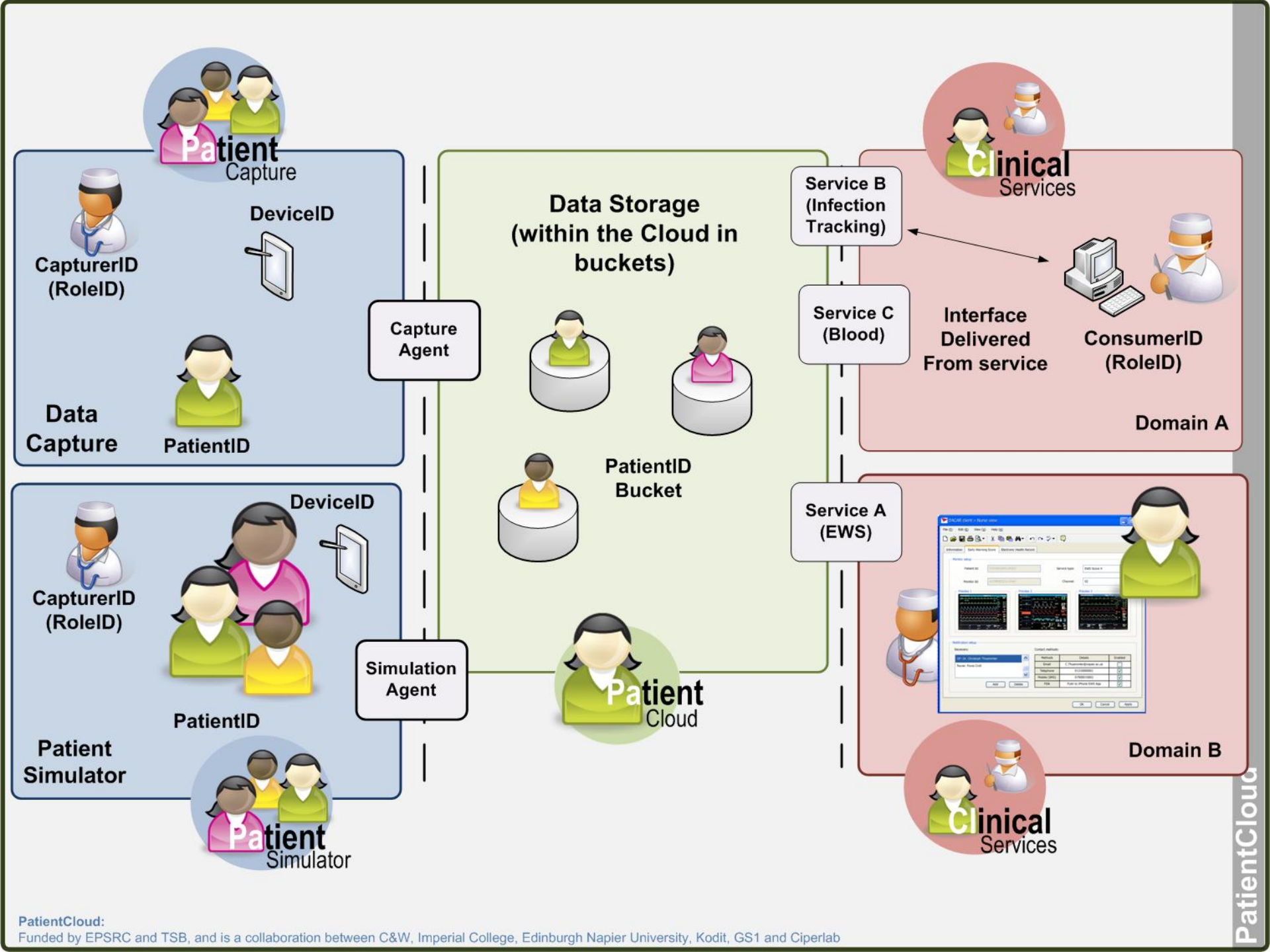
**Dynamic Patient Records**

**Security Policy (including interdomain rights)**

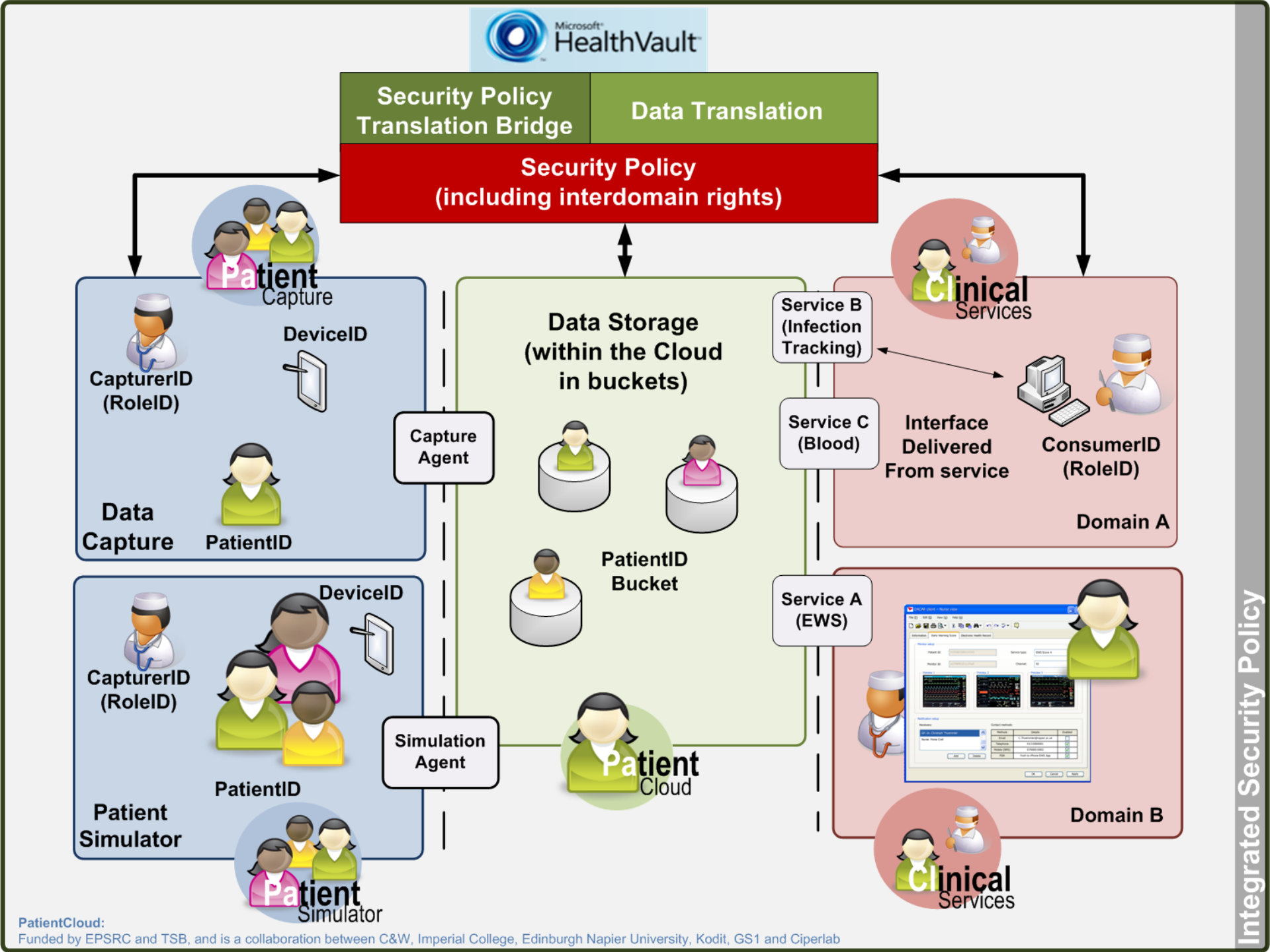


Why?

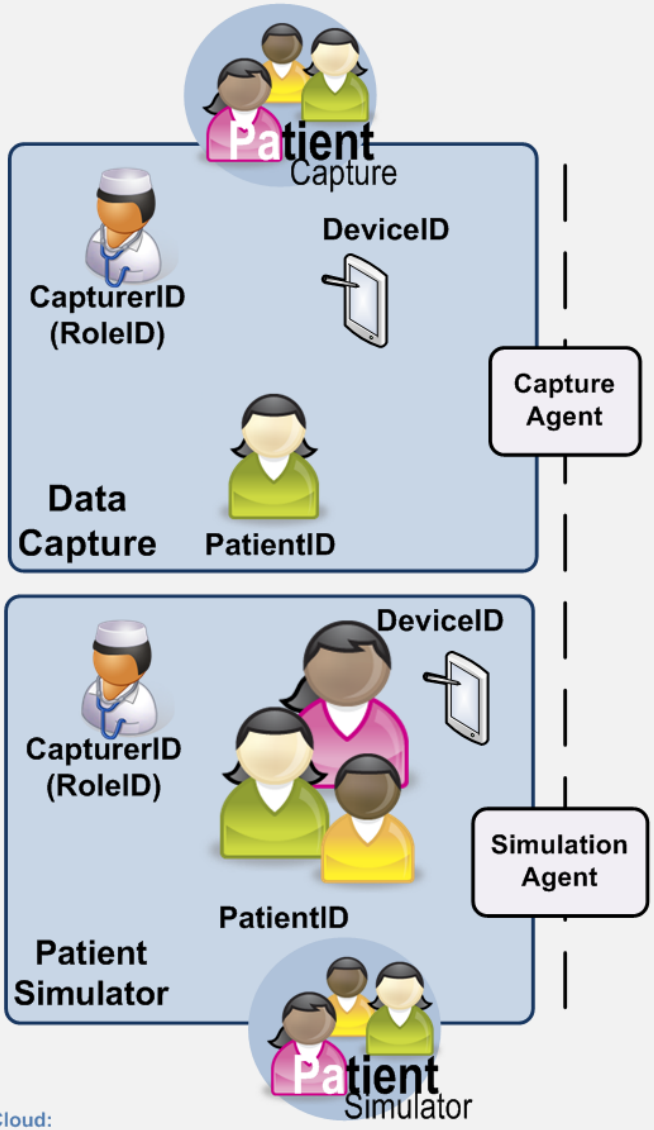
**PatientCloud:**
Funded by EPSRC and TSB, and is a collaboration between C&W, Imperial College, Edinburgh Napier University, Kodit, GS1 and Ciperlab

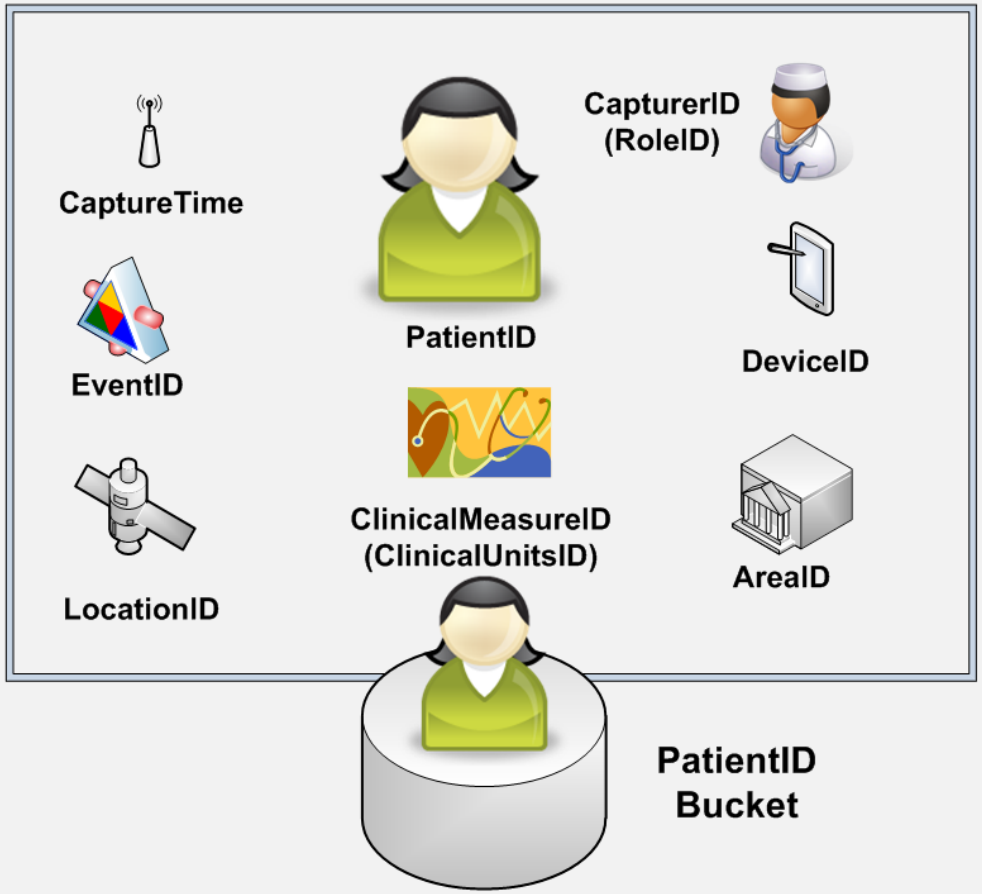


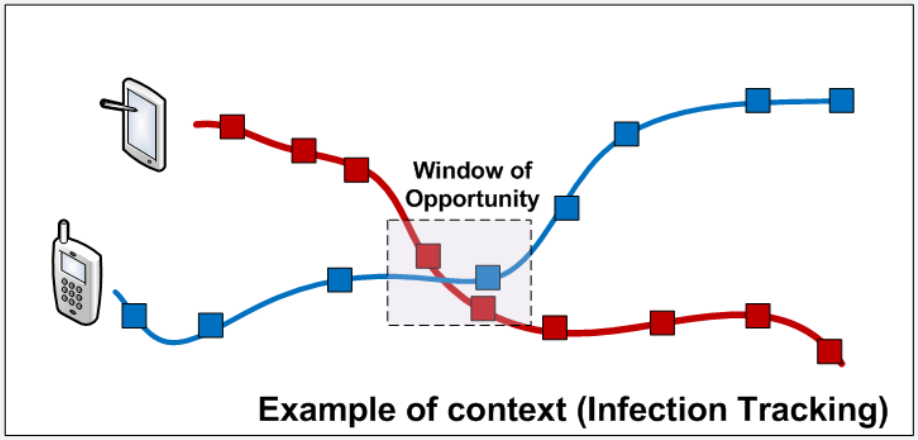

**PatientCloud:**
Funded by EPSRC and TSB, and is a collaboration between C&W, Imperial College, Edinburgh Napier University, Kodit, GS1 and Ciperlab




**PatientCloud:**
Funded by EPSRC and TSB, and is a collaboration between C&W, Imperial College, Edinburgh Napier University, Kodit, GS1 and Ciperlab

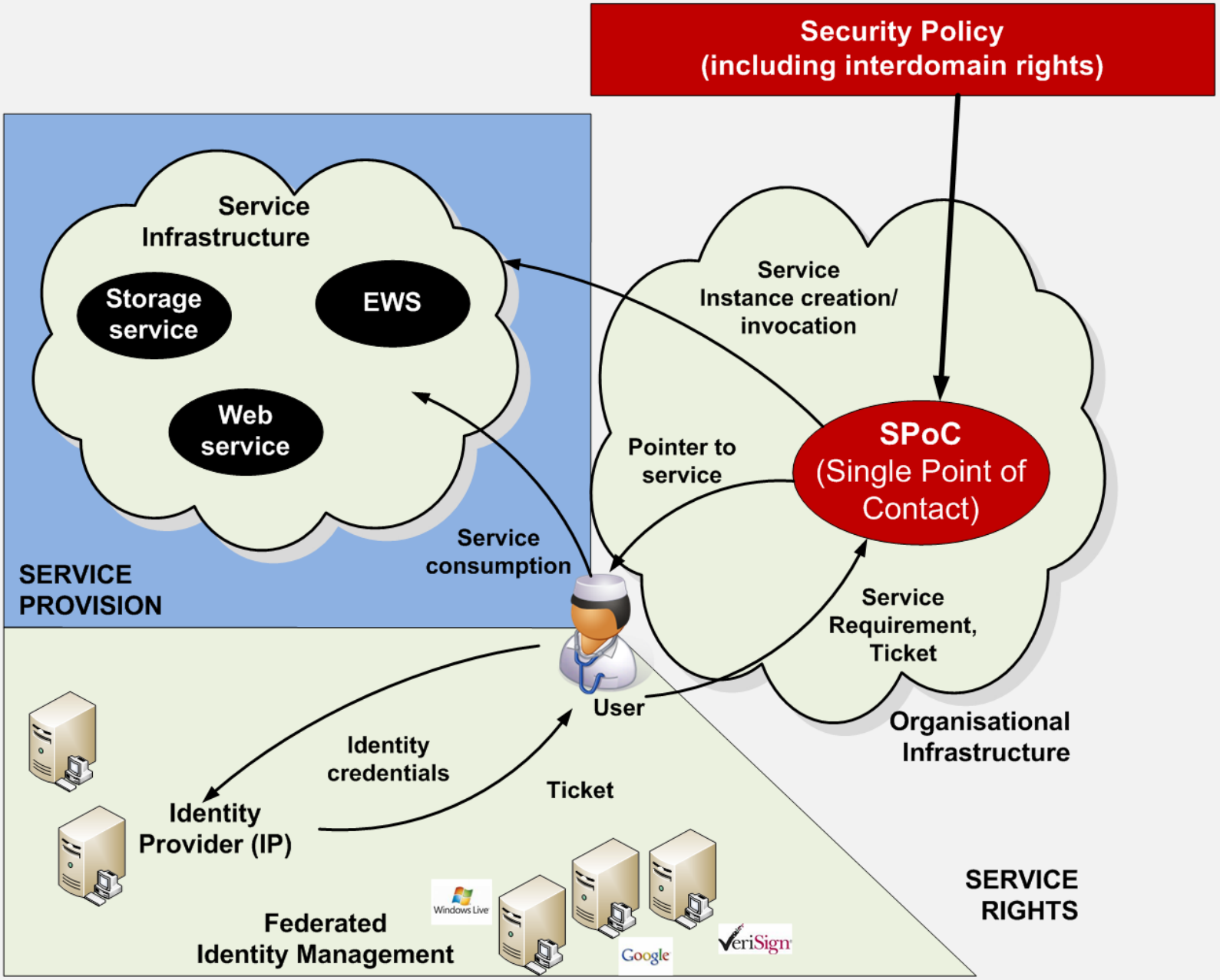


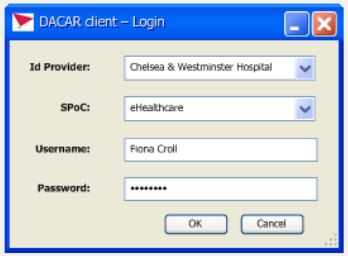



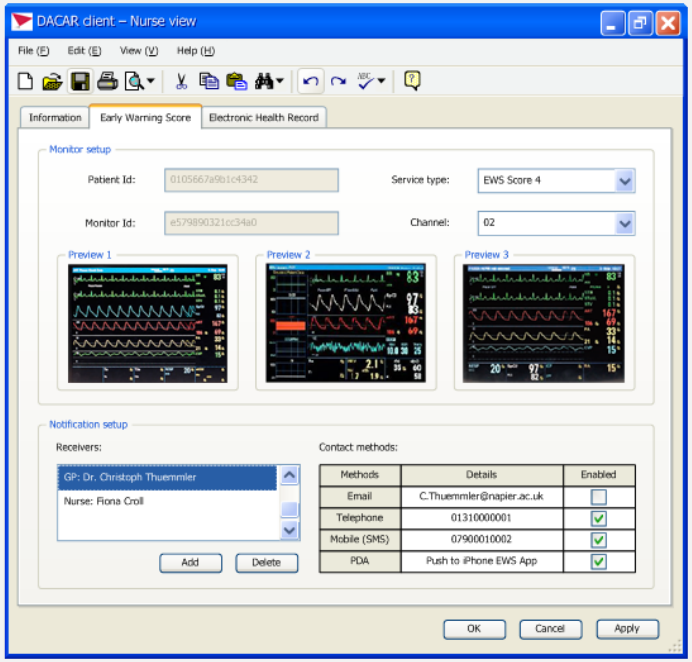

Data Capture Element

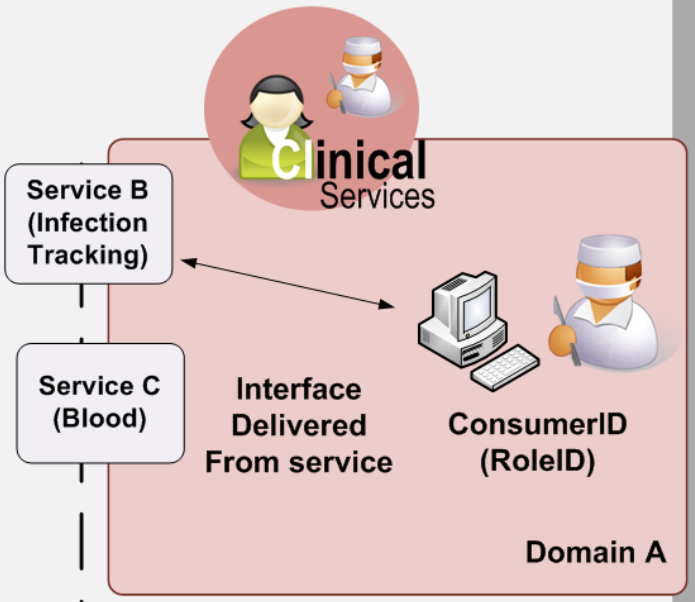
PatientCloud:
Funded by EPSRC and TSB, and is a collaboration between C&W, Imperial College, Edinburgh Napier University, Kodit, GS1 and Ciperlab

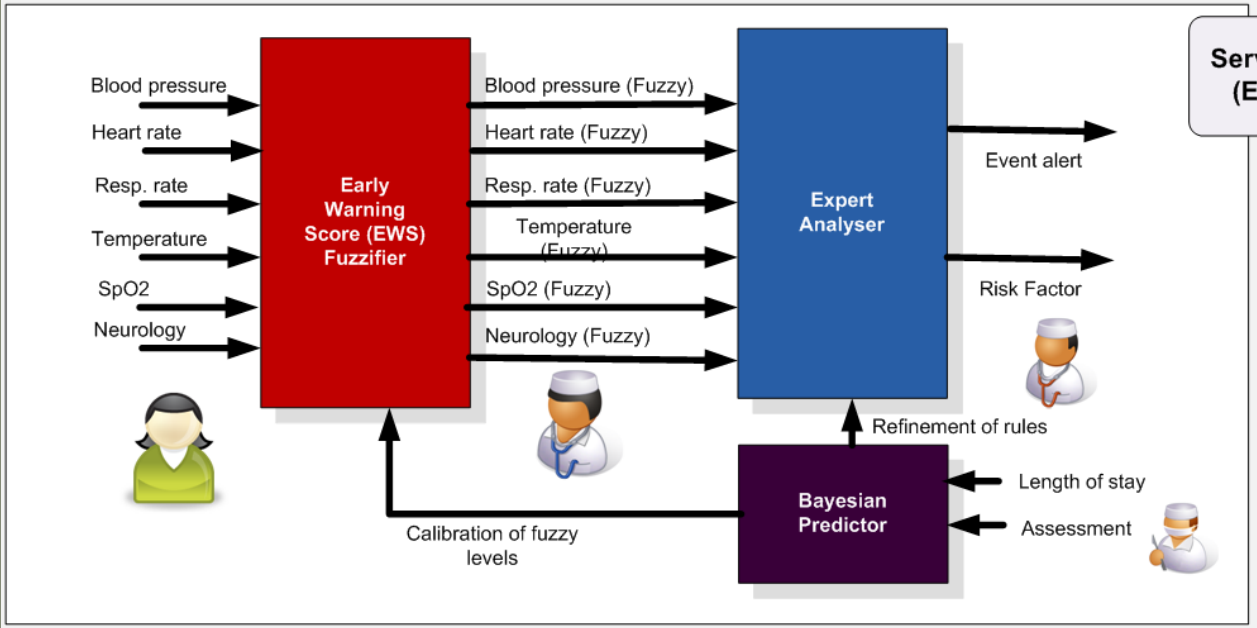


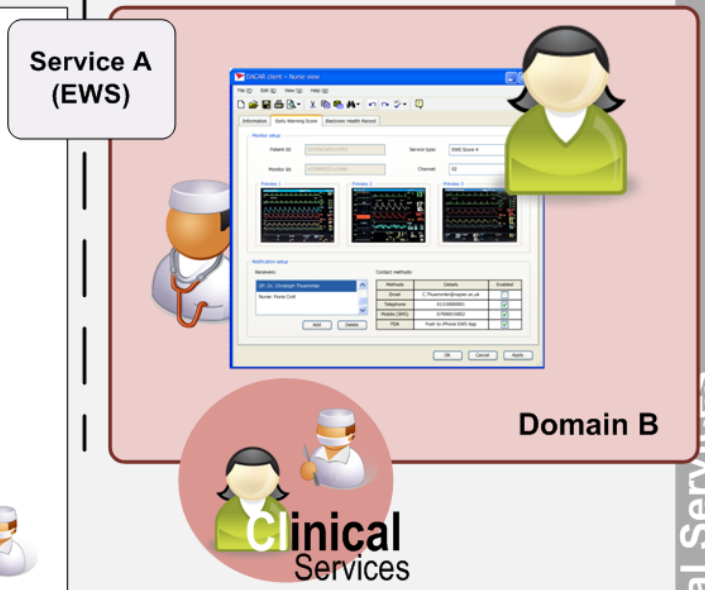

**PatientCloud:**
Funded by EPSRC and TSB, and is a collaboration between C&W, Imperial College, Edinburgh Napier University, Kodit, GS1 and Ciperlab




Clinical Services

**PatientCloud:**
Funded by EPSRC and TSB, and is a collaboration between C&W, Imperial College, Edinburgh Napier University, Kodit, GS1 and Ciperlab

Patient Simulator

Clinical Services

Service B (Infection Tracking)

Service C (Blood)

Interface Delivered From service

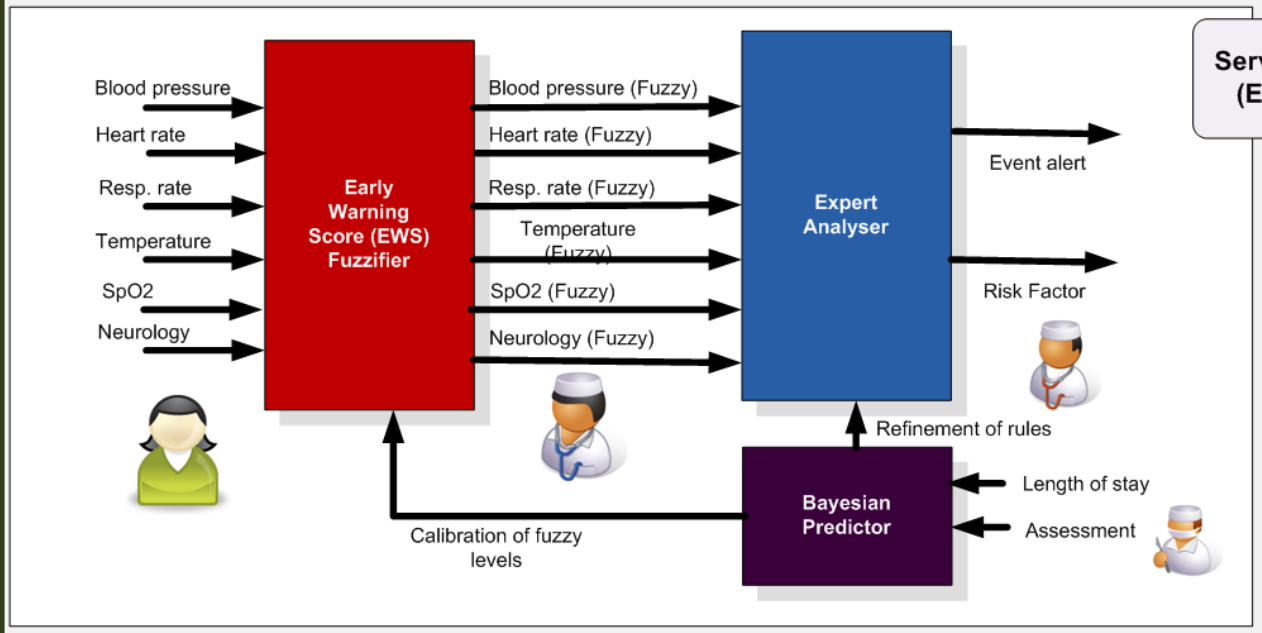
ConsumerID (RoleID)

Domain A

Service A (EWS)

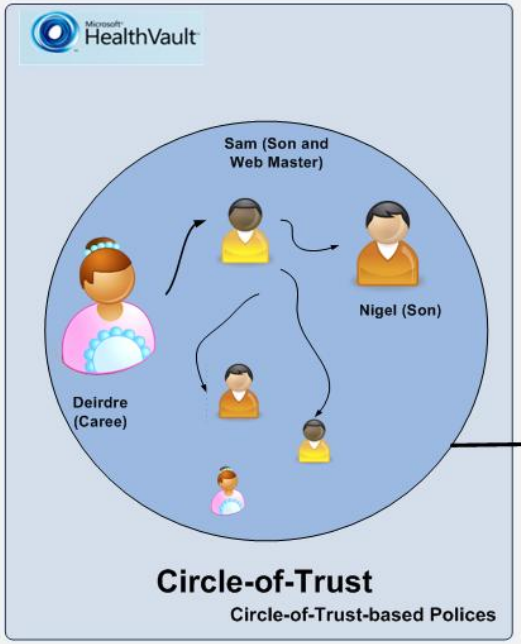
Domain B

Clinical Services



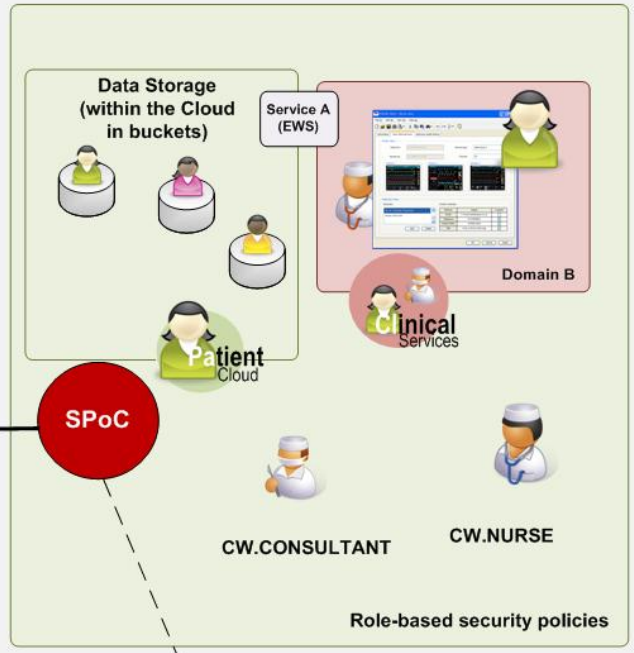

**PatientCloud:**
Funded by EPSRC and TSB, and is a collaboration between C&W, Imperial College, Edinburgh Napier University, Kodit, GS1 and Ciperlab

## Assisted Living




Translation Gateway (Security Policy/ ID Mapping)

## Primary/Secondary Care

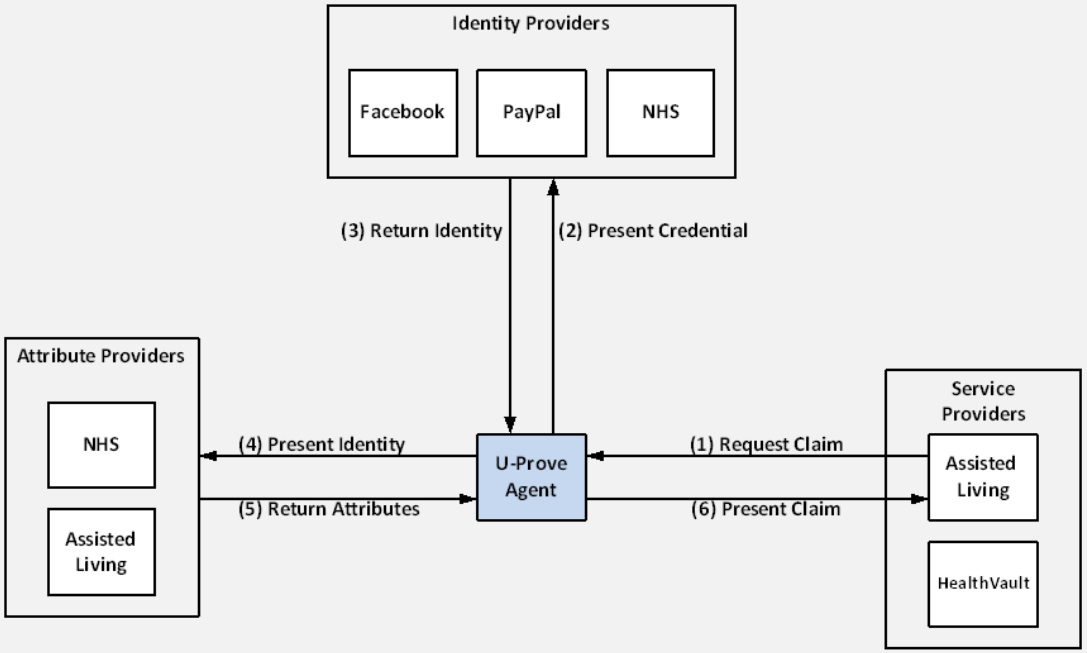


```
[permit] [C&W.NURSE] [C | R] [Temp | SpO2 | HR | BP | RR |
Pain] of [Patient26078] with [EWS] from [Chelsea &
Westminster Hospital] for [*] records in [P2010-12-
30T00:00:00] using [Data Protection Act]

[permit | deny] [Requester] [C | R | U | D] [Attribute] of
[Object] with [Context] from [Owner] for [N] records in
[Time Window] using [Compliance]
```

## Governance Policy

**PatientCloud:**
Funded by EPSRC and TSB, and is a collaboration between C&W, Imperial College, Edinburgh Napier University, Kodit, GS1 and Ciperlab



HealthVault

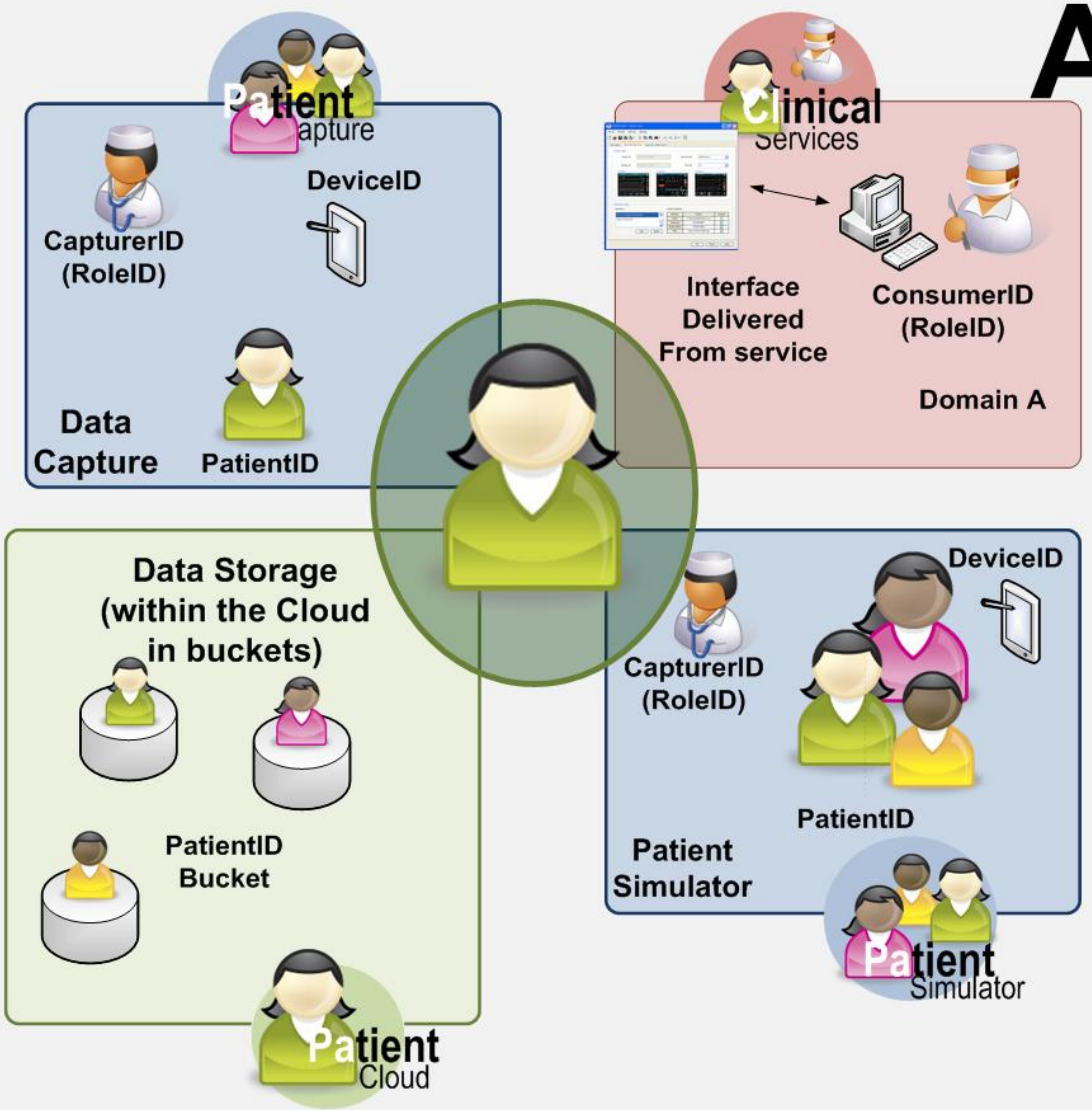
E-Health Platform

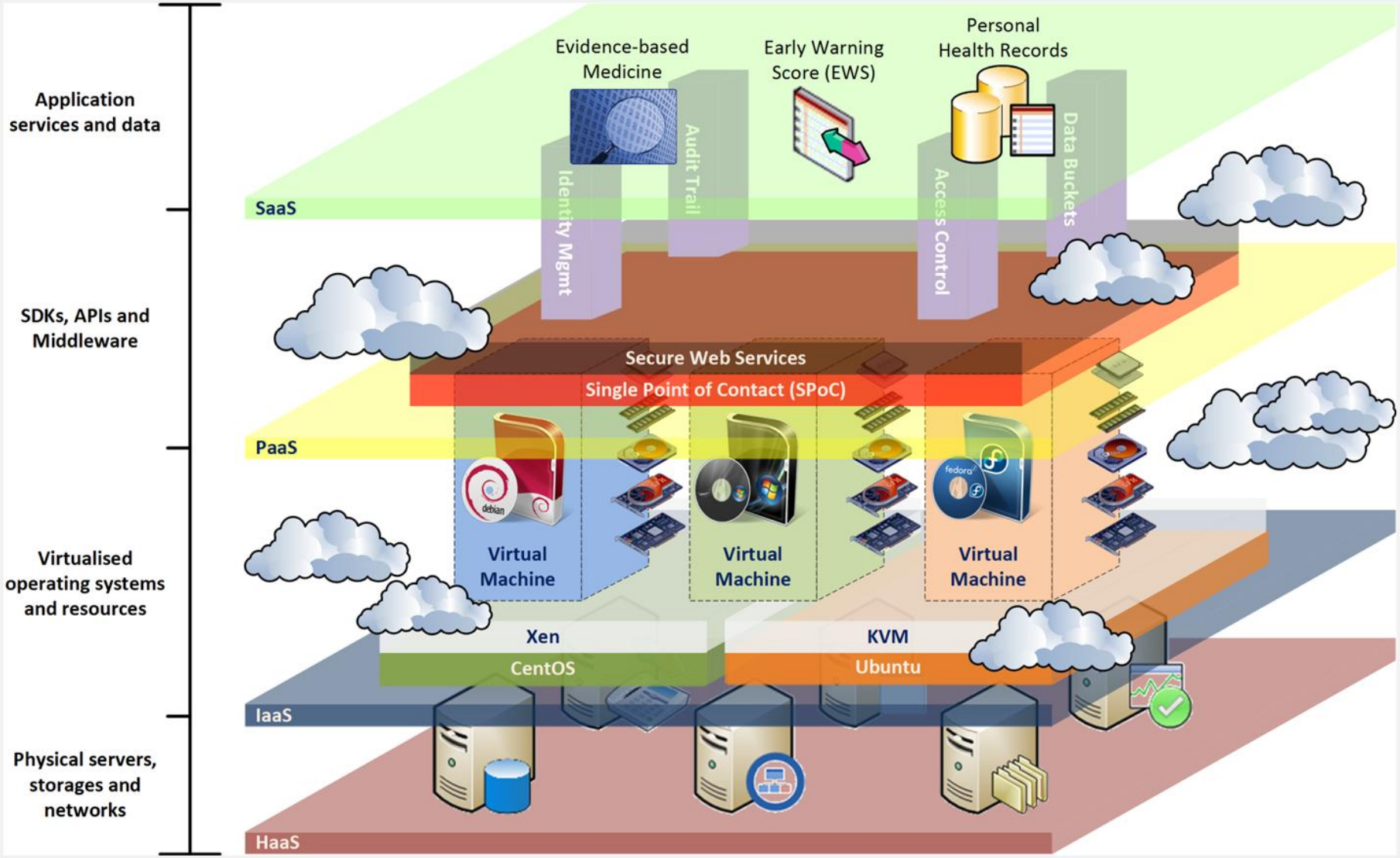
CW.CONSULTANT

CW.NURSE

**PatientCloud:**
Funded by EPSRC and TSB, and is a collaboration between C&W, Imperial College, Edinburgh Napier University, Kodit, GS1 and Ciperlab

# SPoC Architecture





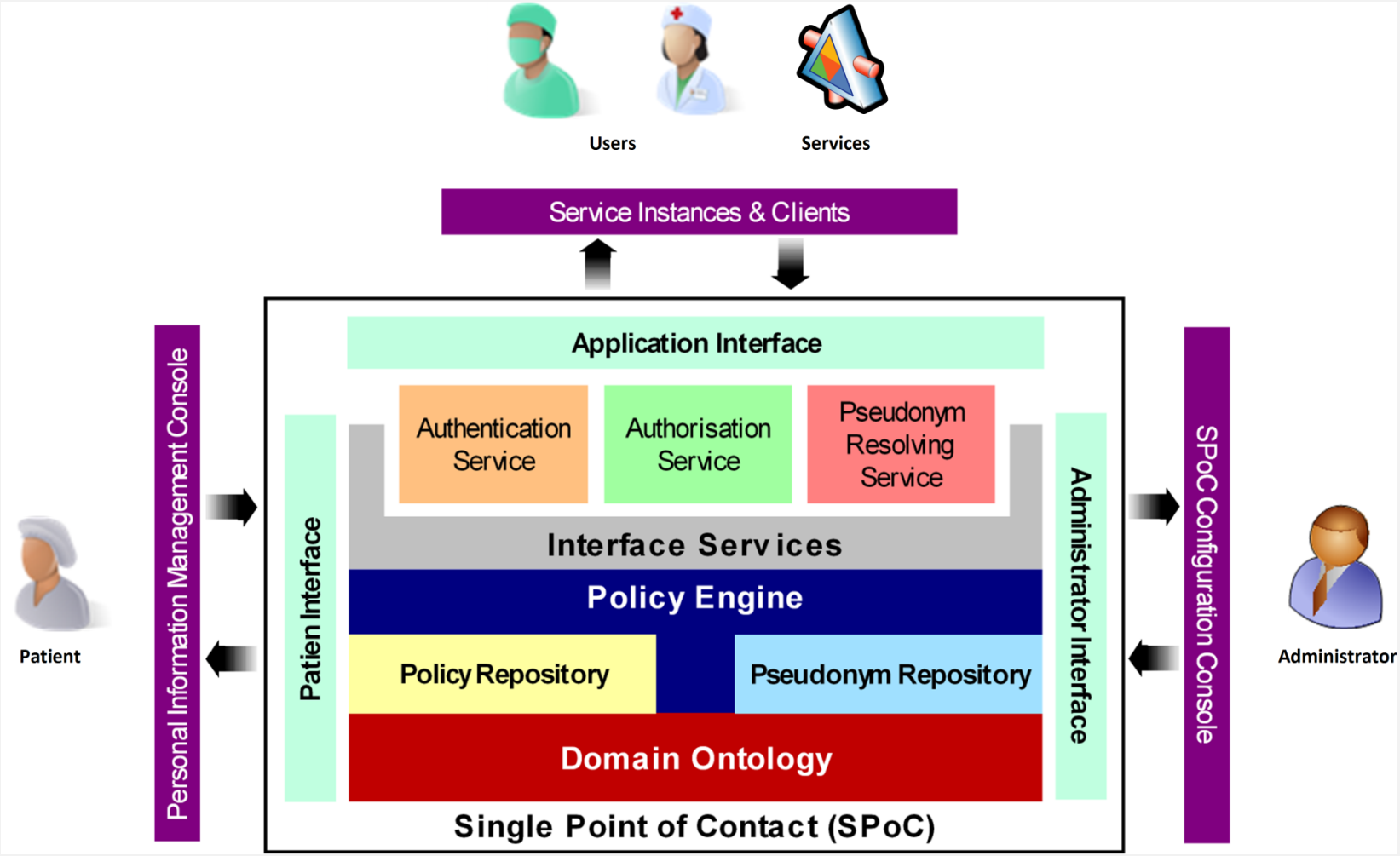

E-Health Platform Architecture

# Single Point of Contact (SPoC)

- A security authority with the following functions
  - Authentication
  - Authorisation
  - Federation
- Claim-based identity management & access control
  - User & Client
  - Claim
  - Security Token Service (STS)
  - Resource Security Token Service (R-STS)
  - Relying Party (RP)

- Authentication
  - Internal users
    - A SPoC may serve as a **STS**
    - A SPoC may be a **RP** of Federated ID Providers
  - External users
    - Each SPoC serves as a **R-STS** in a *SPoCs Federation*
- Authorisation
  - Service authorisation
    - Role- or individual-based access to e-Health services
    - A SPoC issues a *Service Ticket* to an authorised client
  - Data authorisation
    - Role- or individual-based *CRUD* over medical attributes
    - A SPoC issues a *Data Ticket* to an authorised client

# SPoC Architecture



# Policy Syntax

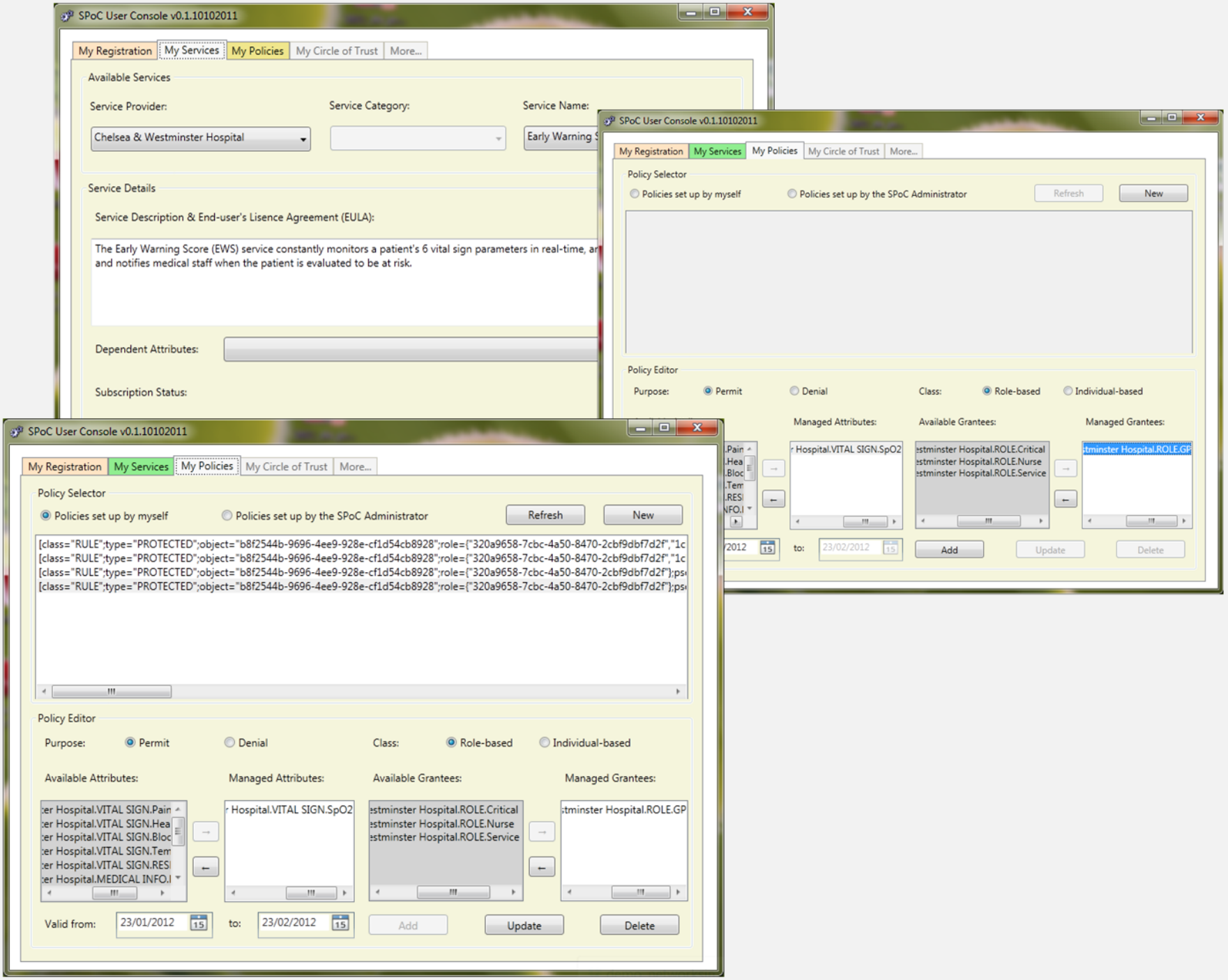
```
[permit] [Medical Staff] [C | R] [Temp | SpO2 | HR | BP | RR | Pain] of
[Patient26078] with [EWS] from [Chelsea & Westminster Hospital] for [*] records
in [P2010-12-30T00:00:00] using [Data Protection Act]

[permit | deny] [Requester] [C | R | U | D] [Attribute] of [Object] with
[Context] from [Owner] for [N] records in [Time Window] using [Compliance].
```

A similar syntax is also applied to the request messages:

```
[Requester] [C | R | U | D] [Attribute] of [Object] with [Context] from [Owner]
within [Start] to [End]
```

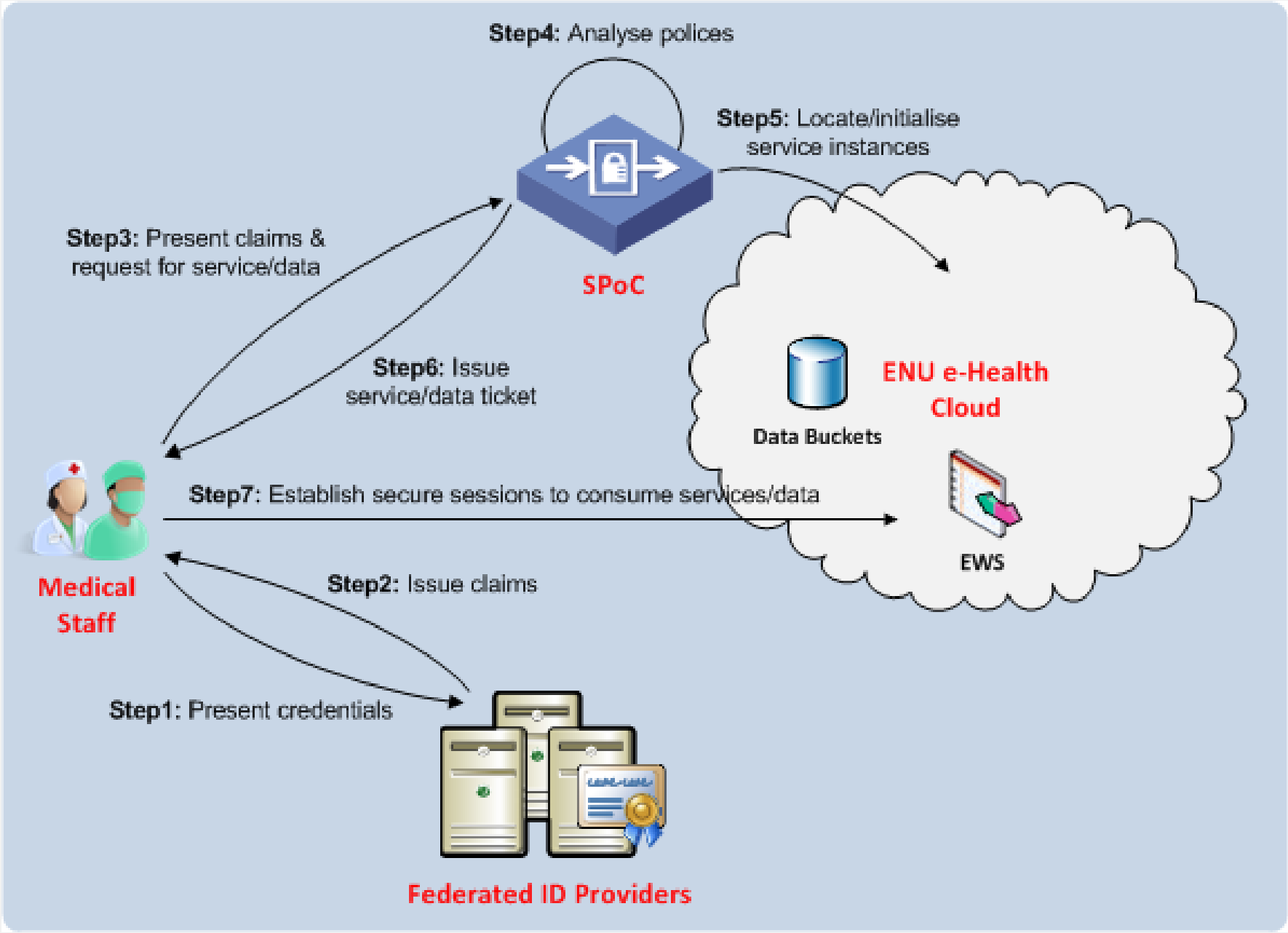
- { [permit | deny] This is part of the rule syntax which indicates the action of the rule. This defines whether a request meeting the rule criteria will be permitted or denied access.
- { [Requester] This identifies a request sender's role, e.g. GP, or pseudonym, e.g. 10420, or a combination of the two, e.g. GP10420.
- { [C | R | U | D] This defines detailed permissions for a requester to create, read, update and delete certain information.
- { [Attribute] This is a unit of information describing an object. An attribute may be a primitive data type, e.g. the pseudonym of an object as a string, or a complex data type, e.g. a person's ECG record for 45 seconds.
- { [Object] This is part of DACAR's system model. It refers to any entities in a healthcare scenario, about which information is held.
- { [Context] This identifies the reason why the information is being shared. The context governs the level of access and permissions associated with information exchange, and hence defines the priority accorded to information requests.
- { [Owner] This species a role with sufficient privileges to manage all aspects of an information source. The owner has the authority to allow or deny access to an information element, as required by legislation and defines responsibilities.
- { [N] records in [Time Window] This defines the number of records permitted over a period of time, where N can be any positive integer.
- { [Compliance] This refers to legislative requirements that support the exchange of information, such as the Data Protection Act, the Human Rights Act, the Freedom of Information Act and so on.
- { [Start] and [End] These identify the start and end of the date/time period over which information shown.

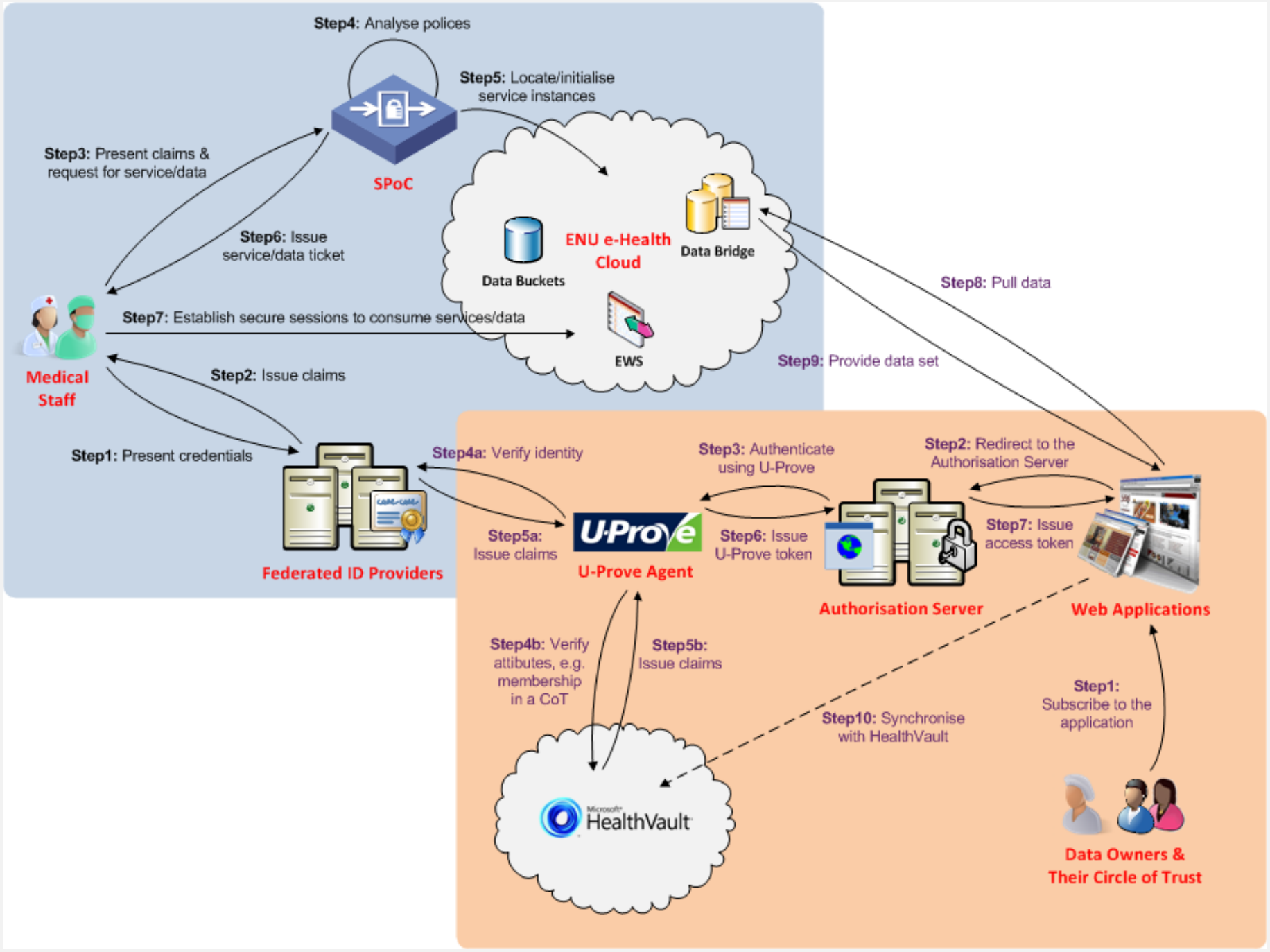



Rights Definition

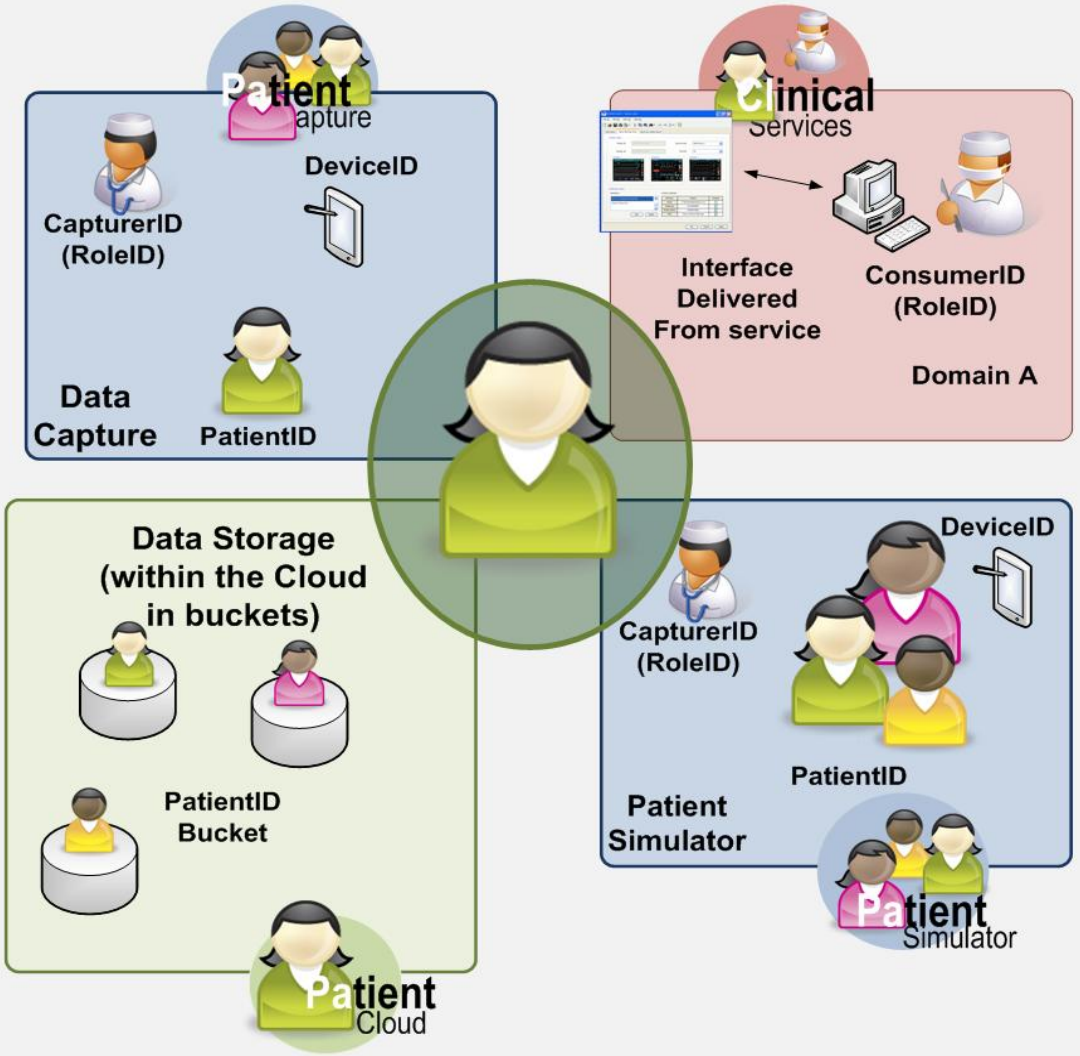
# Policy Categories

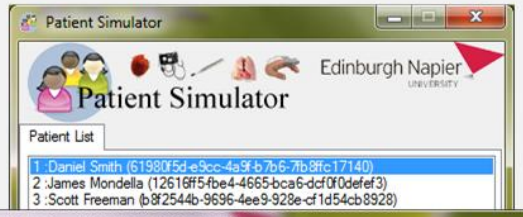
- Service Authorisation
  - To allow or deny certain roles or individuals to consume an e-Health service
- Service Subscription
  - To allow a service to access or modify a set of a patient's medical data in order to perform its functionalities
- Specific Consent
  - To allow or deny certain roles or individuals to access or modify a patient's data in a fine-grained manner
- General Consent
  - To express a patient's willingness to share anonymised medical data in a certain application context

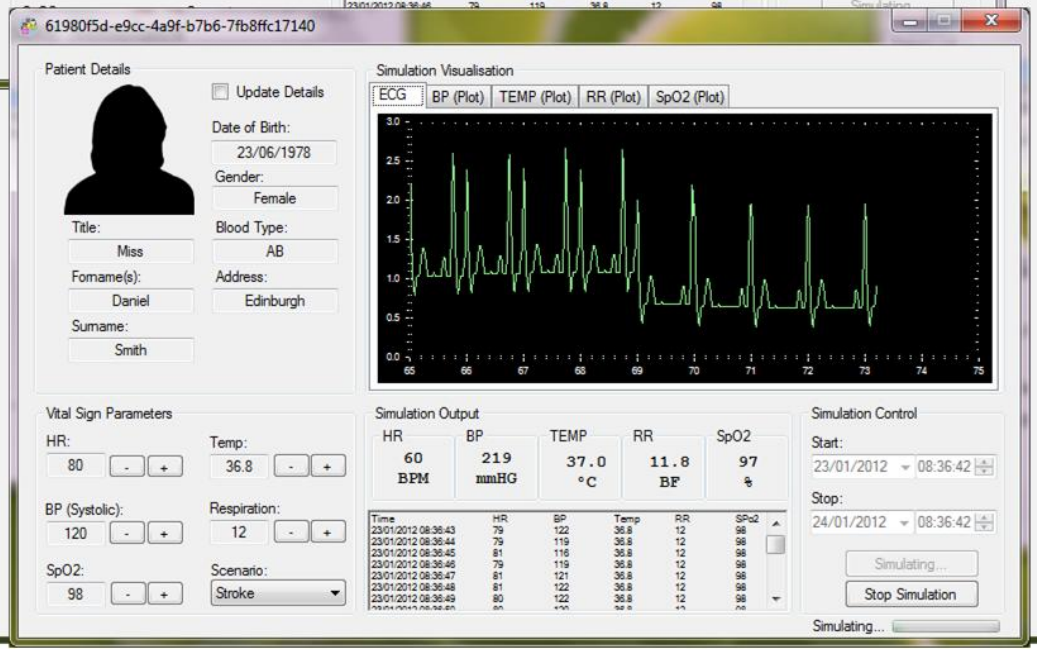

Step4: Analyse polices
Step5: Locate/initialise service instances
Step3: Present claims & request for service/data
SPoC
Step6: Issue service/data ticket
ENU e-Health Cloud
Data Buckets
EWS
Step7: Establish secure sessions to consume services/data
Medical Staff
Step2: Issue claims
Step1: Present credentials
Federated ID Providers

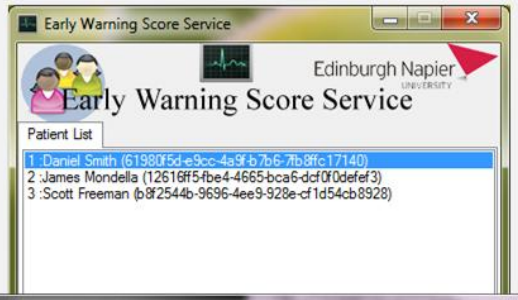

Step4: Analyse polices
Step5: Locate/initialise service instances
Step3: Present claims & request for service/data
Step6: Issue service/data ticket
SPoC
ENU e-Health Cloud
Data Buckets
Data Bridge
EWS
Step8: Pull data
Step7: Establish secure sessions to consume services/data
Step9: Provide data set
Medical Staff
Step2: Issue claims
Step1: Present credentials
Federated ID Providers
Step4a: Verify identity
Step5a: Issue claims
U-Prove Agent
Step3: Authenticate using U-Prove
Step6: Issue U-Prove token
Step2: Redirect to the Authorisation Server
Step7: Issue access token
Authorisation Server
Web Applications
Step4b: Verify attibutes, e.g. membership in a CoT
Step5b: Issue claims
Step10: Synchronise with HealthVault
Step1: Subscribe to the application
HealthVault
Data Owners & Their Circle of Trust
E-Health Platform Architecture

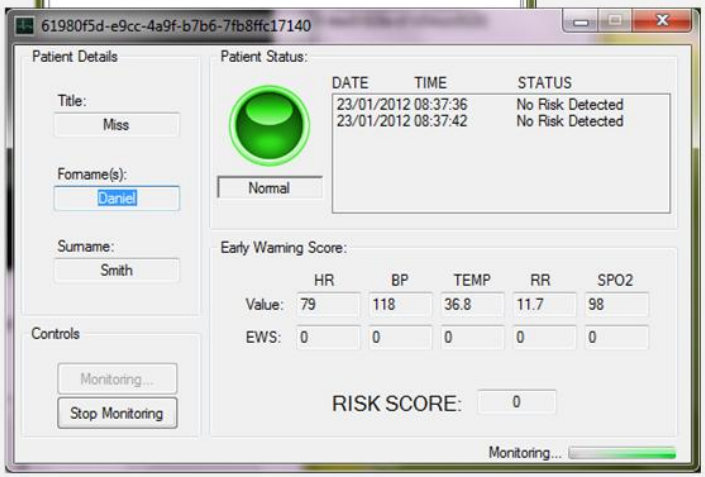
# Patient Simulator

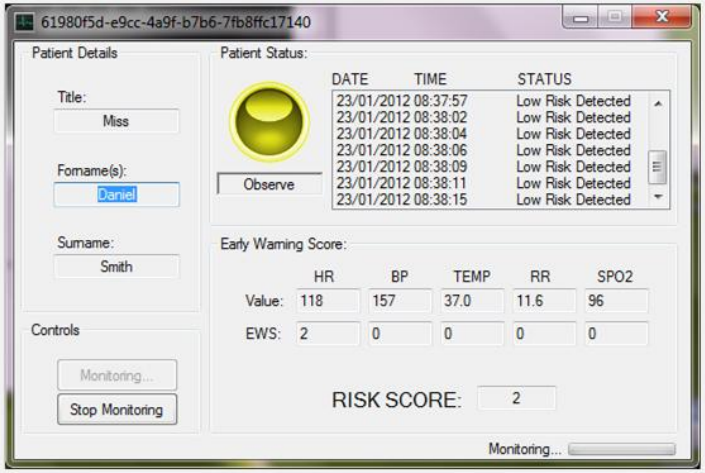






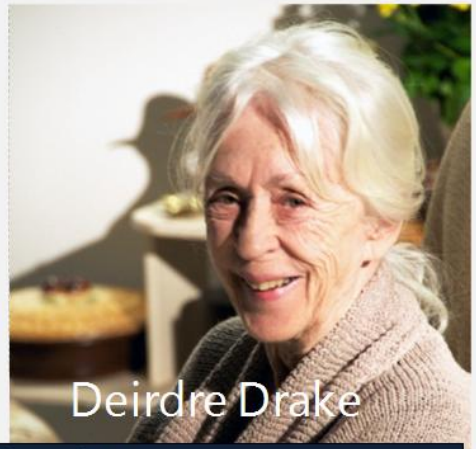

Patient Simulator

ARAB HEALTH ARAB HEALTH CONGRESS
Electronic Healthcare Records Forum 2012

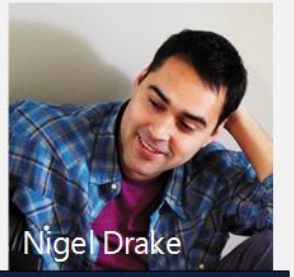
# A Next Generation Cloud-based Health Care Platform

Prof Bill Buchanan, Dr Lu Fan, Prof Christoph Thuemmler, Dr Elias Ekonomou, Owen Lo, and Alistair Lawson, Edinburgh Napier University.

- Healthcare Professional.
- Invited user




- Care Subject
- 82 years old
- House bound
- COPD (Chronic Obstructive Pulmonary Disease)




- Invited user

- GP.
- Invited user

- Site Creator
- Primary Carer

Assisted Living (Informal and Trust based)

Primary Health Care (Formal and role-oriented) - GP

Secondary Health Care (Formal and role-oriented) - Hospitals/A&E

Social Care/Health/etc

**PatientCloud:**
Funded by EPSRC and TSB, and is a collaboration between C&W, Imperial College, Edinburgh Napier University, Kodit, GS1 and Ciperlab