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.
Integrated and Secure Cloud-based e-Health for Holistic Care

- Nurse Kate
  - Healthcare Professional
  - Invited user

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

- Nigel Drake
  - Invited user

- Sam Drake
  - Site Creator
  - Primary Carer

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

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

Social Care/Health/etc

Assisted Living (Informal and Trust based)

PatientCloud:
Funded by EPSRC and TSB, and is a collaboration between C&W, Imperial College, Edinburgh Napier University, Kอดิล, GS1 and Ciperlab
Integrated and Secure Cloud-based e-Health for Holistic Care
Integrated and Secure Cloud-based e-Health for Holistic Care

Some key issues

Societal

- Lack of integration between assisted living, primary and secondary care
- Aging population
- Lack of information sharing across the public sector
- Strong demand to consume health care data
- Lack of integration with careers and trusted people

Technical

- Patient records are often static
- Different systems/formatting used for data
- Limited/difficult access methods ... typically Government infrastructures ... lack of trust
- Poor access control to data
- Data often aggregated and context is often lost

PatientCloud: Funded by EPSRC and TSB, and is a collaboration between C&W, Imperial College, Edinburgh Napier University, Kodit, GS1 and Ciperlab
Manager might ask: What’s the 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?

Primary Health Care (Formal and role-oriented)

Secondary Health Care (Formal and role-oriented)

Assisted Living (Informal and Trust based)

Translation of rights
Translation of identities

Strong Governance Policy
- Often localised
- Different systems/formats
- Poor access control
- Poor identity verification
- Cannot be aggregated
- Etc.
Integrated and Secure Cloud-based e-Health for Holistic Care

Security Policy Translation Bridge

Data Translation

Security Policy (including interdomain rights)

Patient Capture

- CapturerID (RoleID)
- PatientID
- DeviceID

Data Storage (within the Cloud in buckets)

- Service B (Infection Tracking)
- Service C (Blood)
- Service A (EWS)

Clinical Services

- Interface Delivered From service
- ConsumerID (RoleID)
- Domain A

Patient Cloud

- PatientID Bucket
- Simulation Agent

Patient Simulator

- CapturerID (RoleID)
- PatientID
- DeviceID

Clinical Services

- Domain B

PatientCloud:
Funded by EPSRC and TSB, and is a collaboration between C&W, Imperial College, Edinburgh Napier University, Kodit, GS1 and Ciperlab
Integrated and Secure Cloud-based eHealth for Holistic Care

Data Capture
- CapturerID (RoleID)
- DeviceID
- PatientID

Capture Agent
- CaptureTime
- EventID
- ClinicalMeasureID (ClinicalUnitsID)
- LocationID
- DeviceID
- AreaID

Patient ID Bucket

Simulation Agent
- PatientID

Example of context (Infection Tracking)

PatientCloud:
Funded by EPSRC and TSB, and is a collaboration between C&W, Imperial College, Edinburgh Napier University, Kodit, GS1 and Ciperlab
Integrated and Secure Cloud-based eHealth for Holistic Care

Service B (Infection Tracking)

Service C (Blood)

ConsumerID (RoleID)

Domain A

Service A (EWS)

Expert Analyser

Event alert

Risk Factor

Refinement of rules

Length of stay

Assessment

Bayesian Predictor

Calibration of fuzzy levels

Blood pressure
Heart rate
Resp. rate
Temperature
SpO2
Neurology

Blood pressure (Fuzzy)
Heart rate (Fuzzy)
Resp. rate (Fuzzy)
Temperature (Fuzzy)
SpO2 (Fuzzy)
Neurology (Fuzzy)

Domain B

Clinical Services

Interface Delivered From service

PatientCloud:
Funded by EPSRC and TSB, and is a collaboration between C&W, Imperial College, Edinburgh Napier University, Kodit, GS1 and Ciperlab
Integrated and Secure Cloud-based eHealth for Holistic Care

Assisted Living

Circle-of-Trust
Circle-of-Trust-based Policies

Primary/Secondary Care

Translation Gateway (Security Policy/ID Mapping)

Data Storage (within the Cloud in buckets)

Service A (EWS)

Role-based security policies

SPoC

CW CONSULTANT

CW NURSE

Role-based security policies

[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
Integrated and Secure Cloud-based e-Health for Holistic Care

SPoC Architecture
Integrated and Secure Cloud-based eHealth for Holistic Care

ENU eHealth Cloud Architecture

- Application services and data
  - SaaS
- SDKs, APIs and Middleware
  - PaaS
- Virtualised operating systems and resources
  - IaaS
  - Xen, CentOS
  - KVM, Ubuntu
- Physical servers, storages and networks
  - HaaS
- Secure Web Services
  - Single Point of Contact (SPoC)
  - Secure Web Services
  - Personal Health Records
  - Early Warning Score (EWS)
  - Audit Trail
  - Identity Management

- 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]


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.
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
**Step 1:** Present credentials

**Step 2:** Issue claims

**Step 3:** Present claims & request for service/data

**Step 4:** Analyse polices

**Step 5:** Locate/initialise service instances

**Step 6:** Issue service/data ticket

**Step 7:** Establish secure sessions to consume services/data

---

**Medical Staff**

---

**Federated ID Providers**

---

**ENU e-Health Cloud**

---

**SPoC**

---

**Data Buckets**

---

**EWS**

---

**Integrated and Secure Cloud-based eHealth for Holistic Care**
Integrated and Secure Cloud-based e-Health for Holistic Care

Step 1: Present credentials
- Federated ID Providers

Step 2: Issue claims
- U-Prove Agent
- Issue claims

Step 3: Authenticate using U-Prove
- Authorisation Server
- Issue U-Prove token

Step 4a: Verify identity
- Authorisation Server
- Issue access token

Step 4b: Verify attributes, e.g., membership in a CoT

Step 5a: Issue claims

Step 5b: Issue claims

Step 6: Issue U-Prove token

Step 7: Issue access token

Step 8: Pull data

Step 9: Provide data set

Step 10: Synchronise with HealthVault

Medical Staff

ENU e-Health Cloud
- Data Bridge
- Data Buckets

Step 3: Present claims & request for service/data

Step 4: Analyse policies

Step 5: Locate/initialise service instances

Step 7: Establish secure sessions to consume services/data

Step 6: Issue service/data ticket

SPoC

Web Applications

Data Owners & Their Circle of Trust

Subscribe to the application
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.