Next Generation Secure e-Health Platform

- Overview of information sharing.
- SPoC (Single Point of Contact) Principle.
- Information Sharing Context.
- E-Health Platform

Prof Bill Buchanan
Threat:
Data leakage.
Damage.
Abuse.
Vandalism.
Fraud.
Breach of Laws.
Breach of Admin rights.
Etc.
Insider Threat

- Trusted Partner Domain
- Gateway
- Insider threat (Remote Access)
- Governance Policy
- Trust infrastructure
- Assets
- Users
- Organisational Infrastructure
- Data
- Governance Policy (Role-based)

Features:
- Auditing/log.
- Compliance.
- Well-known policy.
- Trust infrastructures.
- Identity/role verification.
- Etc.
Information Sharing

Context

Author: Prof Bill Buchanan
Information sharing

Police domain

Social care domain

Educational Domain

Health care Domain (Primary/Secondary)

Sharing between domains
ILP (Intelligence-led policing) – proactive, researched and planned approach to policing and relies on a robust information-sharing mechanism.

MOPI (Management of Police Information) – best practices for consistent information recording, management and sharing

NIM (National Intelligence Model) – principles for communities to achieve common strategic, tactical solutions to common problems

Author: Prof Bill Buchanan
MOPI

Roles: CI, IS Officer, PC
Roles: Social Worker, IS Officer, Senior Social Worker

Message Syntax

Police domain

Security Policy

Social care domain

SPoC

Roles exposed

Requestor

Owner

Author: Prof Bill Buchanan


- **REQUESTER** = {Social worker, Doctor, Police Inspector...}.  
- **ATTRIBUTE** = {Location, Identity, History, Behaviour, Interaction, Association}.  
- **OBJECT** = Any searchable entity about which information is held and which is mapped to a UID within the domain.  
- **CONTEXT** = {Crisis, Terrorism, Murder, Missing Person, Child/Adult Protection, Drugs, Volume Crime, Petty Crime, General Request}.  
- **OWNER** = {Business Unit 1, Business Unit 2, ...}.  
- **TIMERANGE** = Definition of time.  
- **RECORDS** = {n}.  

Social care domain


Author: Prof Bill Buchanan


Too many records – please refine the search

100 records Return!

Author: Prof Bill Buchanan
Information Sharing

Context


Author: Prof Bill Buchanan
High-level policy (MOPI) → Intermediate Formal Policy → Policy implementation


Author: Prof Bill Buchanan
Next-generation Information Sharing Infrastructure

- Scalable architecture.
- Enhanced security.
- No need to expose data structure to other domains.
- Well defined policies.
- Integrated auditing/compliance.
- Context allows access, if required.
- Lock-down (explicit deny).
- Interchange between any domain.
- Links to any domain.
- Customised policies between domains.
A Next Generation Cloud-based Health Care Platform – Towards Trust and an Infinite Possibilities

Napier: Bill Buchanan, Christoph Thuemmler, Lu Fan, Elias Ekonomou, Owen Lo.
Imperial: Prof Derek Bell

Nurse Kate
- Healthcare Professional
- Invited user

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

Sam Drake
- Site Creator
- Primary Carer

Nigel Drake
- Invited user

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

Static Patient Record

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

Data Storage (within the Cloud in buckets)

- PatientID Bucket
- Dynamic Patient Records

Security Policy (including interdomain rights)

PatientCloud:
Funded by EPSRC and TSB, and is a collaboration between C&W, Imperial College, Edinburgh Napier University, Kodit, GS1 and Ciperlab
Security Policy
(including interdomain rights)

SERVICE PROVISION

Service Infrastructure
- Storage service
- EWS
- Web service

SERVICE RIGHTS

User
- Identity credentials
- Ticket

Federated Identity Management

Identity Provider (IP)

Organisational Infrastructure

SPoC (Single Point of Contact)

Service Instance creation/invocation

Pointer to service

Service Requirement, Ticket

PatientCloud:
Funded by EPSRC and TSB, and is a collaboration between C&W, Imperial College, Edinburgh Napier University, Kodit, GS1 and Ciperlab
[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.
Service B (Infection Tracking)

Service C (Blood)

Interface Delivered From service

ConsumerID (RoleID)

Domain A

Service A (EWS)

Event alert

Risk Factor

Refinement of rules

Length of stay

Assessment

Bayesian Predictor

Calibration of fuzzy levels

Fuzzy Predictor

Blood pressure
Heart rate
Resp. rate
Temperature
SpO2
Neurology

Expert Analyser

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

Domain B

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

---

**Early Warning Score (EWS) Fuzzifier**
- Blood pressure
- Heart rate
- Resp. rate
- Temperature
- SpO2
- Neurology

**Expert Analyser**
- Blood pressure (Fuzzy)
- Heart rate (Fuzzy)
- Resp. rate (Fuzzy)
- Temperature (Fuzzy)
- SpO2 (Fuzzy)
- Neurology (Fuzzy)

**Bayesian Predictor**
- Calibration of fuzzy levels
- Refinement of rules
- Length of stay
- Assessment

**Risk Factor**
- Event alert

**Service A (EWS)**

**Domain A**
- Service B (Infection Tracking)
- Service C (Blood)

**ConsumerID (RoleID)**
- Interface Delivered From service

**Domain B**
- Clinical Services

---


**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)

Domain B

Patient Cloud

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]
Insider Threat

- Trusted Partner Domain
- Gateway
- Governance Policy
- Insider threat (Remote Access)
- Trust infrastructure
- Features:
  - Auditing/log.
  - Compliance.
  - Well-known policy.
  - Trust infrastructures.
  - Identity/role verification.
  - Etc.
- Users
- Assets
- Organisational Infrastructure
- Data
- Governance Policy (Role-based)

BCS

Insider