# Accessing Patient Records in Virtual Healthcare Organisations

Mike BONIFACE[1], Thomas LEONARD[1], Mike SURRIDGE[1], Steve TAYLOR[1]
Leslie FINLAY[2], Declan McCORRY[2]
[1]*IT Innovation Centre, University of Southampton, 2 Venture Road, Chilworth Science Park, Southampton, SO16 7NP, UK*
*Tel: +44 23 8076 0834, Fax: + 44 23 8076 0833, Email:mjb@it-innovation.soton.ac.uk*
[2]*South & East Belfast HSS Trust, Knockbracken Healthcare Park, Saintfield Road, Belfast BT8 8BH*
*Tel: +44 28 9056 5656, Fax: + 44 28 9056 5813, Email: leslie.finlay@sebt.n-i.nhs.uk*

**Abstract:** The ARTEMIS project is developing a semantic web service based P2P interoperability infrastructure for healthcare information systems that will allow healthcare providers to securely share patient records within virtual healthcare organisations. Authorisation decisions to access patient records across organisation boundaries can be very dynamic and must occur within a strict legislative framework. In ARTEMIS we are developing a dynamic authorisation mechanism called PBAC that provides a means of contextual and process oriented access control to enforce healthcare business processes. PBAC demonstrates how healthcare providers can dynamically share patient records for care pathways across organisation boundaries.

## 1. Introduction

The effective delivery of patient care requires that healthcare professionals have access to all relevant information regarding a patient's condition when making decisions. Much of this information may be historic and may have been gathered over many encounters with healthcare providers in different locations using heterogeneous healthcare information systems. Typically, these systems are standalone, developed by many different suppliers and are incompatible with one another. The lack of integration between departmental, hospital and regional information systems in terms of well-defined business processes produces serious inefficiencies when delivering patient care [1].

Government agencies, healthcare providers and systems vendors have various initiatives for integrating the healthcare enterprise; however, most strategies are based on centralising resources within an enterprise at the level of healthcare provider or healthcare region. For these reasons sharing patient electronic patient records across the borders of organisations is rarely achieved today. For example, the NHS IT programme in England is creating a NHS care record service that accesses clinical information held on a national database called the SPINE [2]. This service will only available in England and other UK regions have different strategies, which will make accessing patient data across all UK regions difficult. IHE have published the XDS: Cross-enterprise document sharing integration profile that provides a technical architecture for sharing patient records but security and privacy requirements are beyond the scope of their analysis [3].

In the ARTEMIS project [4], [5] we are developing a semantic web service based P2P interoperability infrastructure for healthcare information systems that will support new ways of providing health and social care. Healthcare providers join an ARTEMIS network

that supports virtual healthcare organisations where patient records are generated and maintained by autonomous healthcare providers and accessed using medical web services. In this paper, we describe the characteristics of virtual healthcare organisations and a supporting infrastructure for dynamically authorising access to stateful healthcare resources within the constraints of data privacy regulations.

## 2. Virtual Healthcare Organisations

Virtual organisations can be defined as flexible, secure and coordinated resource sharing amongst dynamic collections of individuals, organisations and resources, in order to achieve a common purpose [6]. In healthcare, virtual organisations allow clinical staff and healthcare providers to collaborate with the objective of delivering patient care through the sharing of patient records and healthcare services. The lifecycle, structure and dynamics of a virtual organisation should be defined based on the business needs of its participants. However, existing infrastructure technologies tend to provide support for virtual organisations with constrained characteristics that are not well matched to the healthcare domain. Exploring how healthcare providers currently share services and patient records across organisational boundaries within the constraints of data privacy legislation provides us with important insights into the infrastructure capabilities required to support a virtual healthcare organisation.

Patient referrals are the key entry point to healthcare systems that allow intra- and inter-enterprise collaboration in the delivery of patient care. Referrals allow care pathways to be created between primary care providers, specialists, labs and other healthcare organisations. For example, a referral may be as simple as a physician sending a patient to another physician for a consultation or it may be as complex as a primary care provider sending a patient to a specialist for specific medical procedures to be performed and attaching the payer authorisations for those requested procedures as well as the relevant clinical information on the patient's case [7].

Each referral represents a specific pathway through a healthcare organisation and consists of a series of administrative and medical tasks. Healthcare professionals are authorised to carry out specific tasks assigned to them. Clerical officers may perform registration and booking whereas consultants may assess a patient’s condition and place appropriate orders. The authorisations to undertake referral tasks are dynamic and depend upon the overall referral state. For example, a consultant may be authorised to assess a specific patient only when an appointment has been scheduled. Within the context of a referral, healthcare professionals are responsible for controlling access to the data they generate. The consultant may then update the patient record following an assessment and delegate access to parts of the record to another doctor as necessary.

Healthcare providers operate within a strict regulatory framework that is enforced to ensure the protection of personal data and outlines conditions and rules in which processing is allowed. There are many such regulations at European level [8] and additional legislation implemented within member states [9]. According to EU Directive 95/46/EC, if a healthcare provider maintains personal data on its patients, the healthcare provider is identified as a data controller and is responsible for protecting that data against unauthorised use. If a healthcare provider wants to access personal data within another organisation they are identified as a data processor. For the communication to occur between data controller and data processor consent must be obtained from the patient and a contract between the two parties must exist that defines the scope of access to patient data including conditions such as what data is to be accessed, what use will be made of the data and how the data will be accessed.

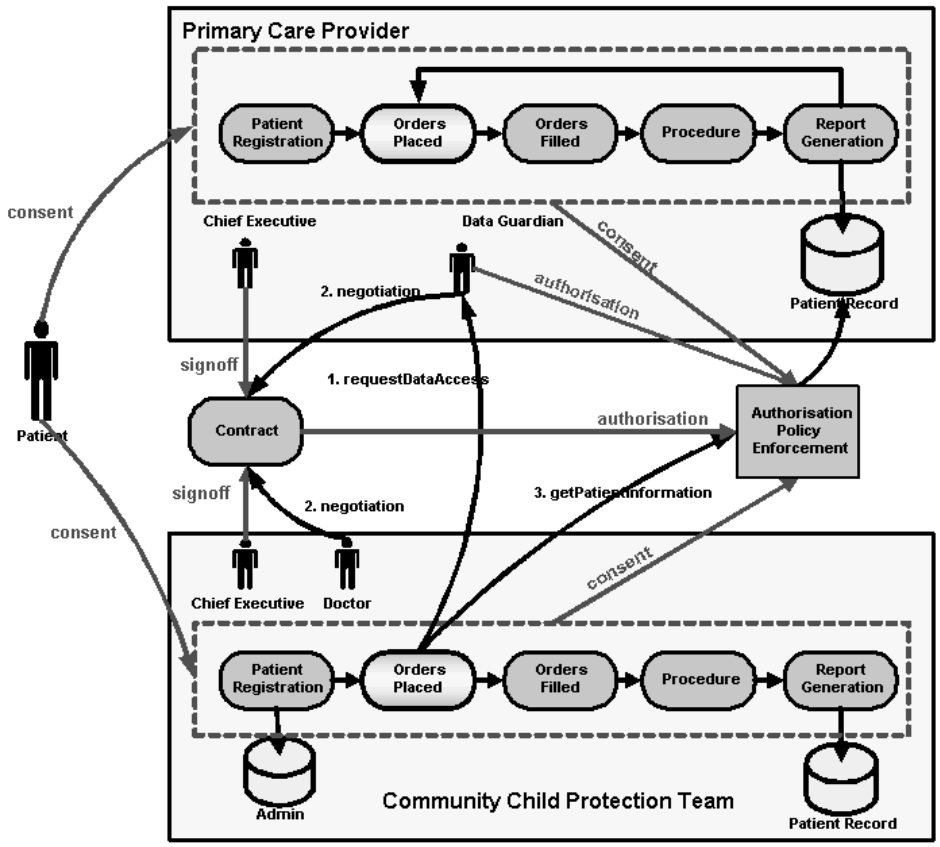


*Figure 1. Healthcare business process for data access negotiation*

Currently, healthcare providers implement an out-of-band business process that permits negotiation of data access agreements. Figure 1 shows an example business process based on an analysis of how South East Belfast Healthcare NHS Trust negotiate data access agreements within the constraints of the UK data protection act. To access patient records an external organisation has to request access by contacting a data guardian within the trust. The data guardian is an individual that is responsible for controlling access to patient data across the boundaries of an organisation. This may include requests from other healthcare providers or requests from patients to see their own records.

For access requests from other healthcare providers there are typically two circumstances, single requests to access data on a specific patient or longer-term requests for agreements to collaborate in the delivery of patient care. For requests to access specific patient records the data guardian should ensure that patient consent has been given before data is shared. The consent allows a patient to express privacy preferences regarding their data defining which organisations are authorised to access the data and for what purpose (e.g. the referral context). In exceptional circumstances, for example, if a patient is unconscious during an emergency episode, the data guardian can authorise access if they decide access is in the best interest of the patient. For longer-term collaborations a contract would be negotiated that is signed by a senior representative of each organisation such as the Chief Executive.

The existing business processes show that collaborations between healthcare providers are very dynamic and represented as bi-lateral data access agreements between data controller and data processor. Healthcare professionals need to share detailed information regarding the person's condition when making decisions during tasks such as referral acceptance and patient assessment. In addition, patient consent should form part of authorisation decision, however, as with most healthcare situations there may be circumstances where human judgement needs to override. ARTEMIS is developing a

dynamic authorisation mechanism called process-based access control to meet the requirements described above supporting healthcare business processes within virtual healthcare organisations.

## 3. Process-based access control

The Process-based access control (PBAC) implementation builds on concepts developed by GRIA, a secure web service grid infrastructure for B2B service provision [10]. It provides a means of process-oriented access control to enforce a business processes associated with a stateful resource model. We define a process as an identifiable sequence of operations on a stateful service. An instance of a process is identified by its *Process Context*. Typically, the Process Context is a reference ID presented to the service. The service uses this ID to retrieve the process identified by the Process Context, and can thus determine the position in the business process, and use this to make authorisation decisions.

Process-based authorisation is grounded in the service's Web Service interface. Unguarded, a Web Service interface is a collection of operations that may be executed by anyone at any time. PBAC dynamically permits and denies access to these operations based on:

- the user making the request;
- the state of the process referred to by the user; and
- the operation requested by the user.

A Process Context ID refers to an instance of a Resource Type. Each Resource Type has a static policy, describing its state model, the permissible state transitions, a set of operations, a set of Process Roles (different user types essentially), and finally a set of permissions that conjoin a state, an operation and a Process Role.

In addition to the Resource Type static policy, PBAC has a dynamic policy, which acts like a repository of information regarding the access decision for a process acting on a particular Resource Type. This holds information such as the current state of a process, and which users have which *Process Roles*. Together the static and dynamic polices make up the entire authorisation decision.

The operations themselves may influence the state of the service. This means there is no need for a meta-policy controlling who can update policy. Services operations may update the state of a process, change criteria defining which subjects can take which Process Roles, and create new Process Contexts.

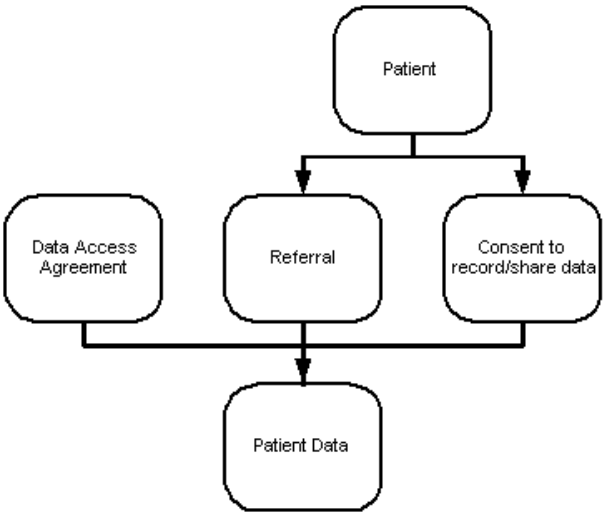


*Figure 2. Healthcare resource model*

Figure 2 shows the resource model used by the ARTEMIS infrastructure. The model contains the following elements:

- **Patient**, used to denote an individual patient
- **Data Access Agreement**, used to encapsulate a trust relationship between a referring healthcare organisation (data processor) and the healthcare organisation that maintains the data (data controller)
- **Consent**, used to encapsulate a trust relationship between a patient and a healthcare organisation
- **Patient Referral**, used to encapsulate an entire workflow for a specific care pathway provided by a healthcare organisation
- **Patient Data** identifiers, used to denote patient record data generated within a referral context

Process contexts can be hierarchical or based on complex rendezvous. For example, in Figure 2 a patient context is created when a healthcare provider registers the patient and referrals and consent (including the patient's privacy preferences) are represented as sub-contexts of the patient's registration. However, when a healthcare provider wants to access a *getPatientInformation* service from another provider, PBAC requires a rendezvous of data access agreement and consent relating to the original referral context before authorisation can be made.

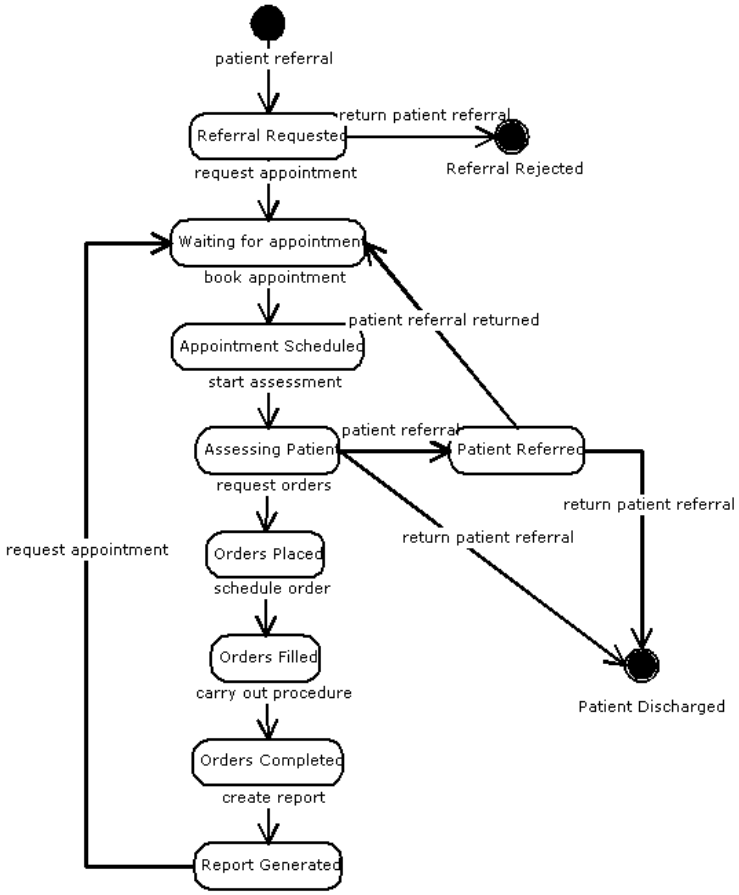


*Figure 3. Patient referral business process*

For each resource defined in Figure 2 a process model has been developed. Figure 3 shows the process model for a patient referral. The process describes possible referral states such as "Referral Requested" and "Appointment Scheduled" along with permissible service operations that can cause state transitions. When the patient referral service operation is

invoked a new Process Context is created for the referral. Healthcare professionals that are assigned to the referral are allocated Process Roles that define permitted actions and associated state transitions. For example, when the Process Context is created a clerical officer may be allocated an Process Role that only allows them to book appointments whereby a consultant once an appointment is scheduled would be able to start assessment, request orders and refer the patient to other healthcare providers.

## 4. PBAC Architecture

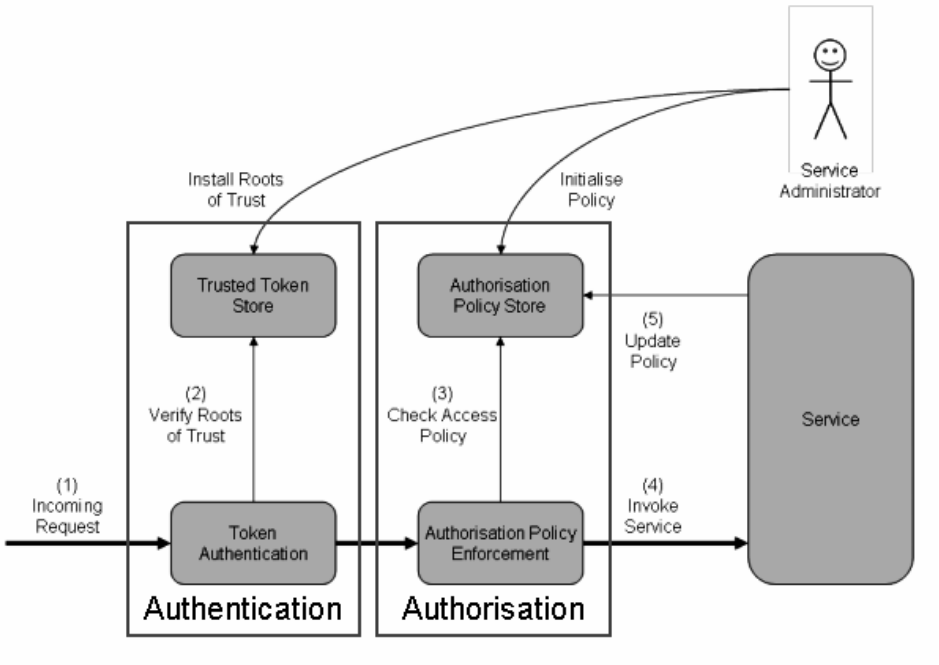


*Figure 4. PBAC Architecture*

Figure 4 shows the high-level architecture of PBAC and how it can be deployed to provide dynamic authorisation for web services. The implementation is based on Apache Axis handlers that intercept incoming service request. We have a clear two-stage operation sequence for access control. Firstly, the client attributes are authenticated taking into account the roots of trust within the WS-Security handler [11]. We take "authentication" to mean that the message is checked for integrity (it has not been altered or tampered with and that it comes from a known client), the client is identified using attributes in their X.509 certificate, and the service that PBAC protects trusts the issuer of the client's certificate to correctly perform the identity checks and issue the certificate. This is a mature process using PKI-based technology and operational procedures, and does not merit discussion here.

The second stage of the process is authorisation. Once authenticated, the message is passed to the authorisation policy enforcement point. The enforcement point then checks the access policy by providing the attributes, operation and current context to the authorisation policy store. If the client is authorised to perform the operation within the current context the service is then invoked. Finally, if necessary the service can update the state of a process, delegate Process Roles to other users, and create new Process Contexts.

## 5. Pilot Application Scenario

An ARTEMIS pilot application is being deployed by healthcare providers located in two European countries to demonstrate the interoperability of healthcare information systems across organisational and country boundaries. The pilot application includes healthcare

providers South East Belfast Healthcare Trust (SEBT) in Belfast, Northern Ireland and Hacettepe Hospital in Ankara, Turkey. Each healthcare provider operates within distinct legislative domains and has different healthcare information systems to support patient care [12], [13].

The clinical scenario focuses a Belfast businessman who is admitted to Hacettepe hospital on a business trip to Ankara in Turkey. The businessman has an ongoing heart condition and is receiving treatment in Belfast from the SEBT District Nursing team following an episode in a Belfast Acute hospital. The assessing doctor knows the patient is from Northern Ireland and searches the ARTEMIS network for healthcare providers within Northern Ireland that hold records for the patient using a patient record discovery protocol [14]. Once patient records have been located at SEBT, the doctors at Hacettepe hospital negotiate a data access agreement (DAA) with the SEBT data guardian using the electronic healthcare record management service. The doctor can then directly request specific documents such as the assessment, case notes and medication record defined in the DAA by quoting the DAA Process Context ID when invoking the Retrieve Information for Display service.

Both healthcare providers and healthcare information system vendors are evaluating PBAC as part of the ARTEMIS pilot application in accordance with ISO 14598 [15]. These stakeholders offer different evaluation perspectives that will enable PBAC to be validated against a wide range of criteria to ensure its suitability for authorisation within a service-based virtual healthcare environment. SEBT is evaluating PBAC from a usability perspective, for example, validating how complex authorisation decisions can be supported in accordance with existing security policies and measuring the reduction in cost and time in creating data access agreements through dynamic authorization compared with existing out-of-band procedures. TEPE is evaluating PBAC from a technical perspective to validate that the architectural approach (static policies, Process Roles) can be easily integrated with existing healthcare information systems without affecting key characteristics such as performance, reliability and maintainability.

## 6. Conclusions

In this paper, we have presented a dynamic authorisation mechanism called PBAC that is being developed within the ARTEMIS project to support business processes in virtual healthcare organisations. PBAC provides a means of contextual and process oriented access control to enforce a business processes associated with a stateful resource model accessed through web service operations. PBAC demonstrates how healthcare providers can dynamically share patient records for care pathways across organisation boundaries.

PBAC offers significant benefits to healthcare providers including:

- Ability to provide complex authorization decisions at a service level based on resource state, contracts and patient consent in accordance with business processes.
- An improved availability of patient data during assessments by providing access to a virtual healthcare record, removing the need for retrospective analysis
- Reduction in cost and time in creating data access agreements through dynamic authorization compared with existing out-of-band procedures

The initial evaluation is focusing on specific healthcare professionals using a limited collection of web services accessing patient data to support the pilot application scenario. However, in practice healthcare systems are typically complex with rich data sets accessed by hundreds of users. In these circumstances, the service provider may need to develop static policy and associated Process Roles for many resource types depending upon the business needs. Future work will extend the pilot application to incorporate a wider range of resource types allowing the scalability and maintainability of PBAC to be validated. Tooling to ensure rapid development of service policies will be developed. In addition,

future work will seek to standardise PBAC interfaces and policy language by implementing and contributing to standards such as WS-Policy [16] and WS-Trust [17].

## References


[1] N. Outram et al, Workshop on Biomedical Informatics and collaboration with the Research Infrastructure projects Report, 18-19 March, Brussels
[2] NHS National IT Programme, http://www.dh.gov.uk/PolicyAndGuidance/InformationPolicy/NationalITProgramme/fs/en
[3] IHE, "IHE Infrastructure Technical Framework Supplement 2004-2005, Cross-Enterprise Document Sharing (XDS), Trial Implementation Version", 15 August 2005, http://www.rsna.org/IHE/tf/IHE_ITI_Cross-enterprise_Doc_Sharing_2004_08-15.pdf
[4] Artemis Project, http://www.srdc.metu.edu.tr/webpage/projects/
[5] Dogac, A., Laleci, G., Kirbas, S., Kabak, Y., Sinir, S., Yildiz, A., "Artemis: Deploying Semantically Enriched Web Services in the Healthcare Domain", Information Systems Journal (Elsevier) special issue on Semantic Web and Web Services, accepted for publication
[6] I. Foster, C. Kesselman, S. Tuecke., The Anatomy of the Grid: Enabling Scalable Virtual Organizations, http://www.globus.org/research/papers/anatomy.pdf
[7] Health Level 7 (HL7), http://www.hl7.org
[8] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L, 23 Nov. 1995, http://europa.eu.int/com-m/internal_market/privacy/law_en.htm
[9] Data Protection Act 1998, UK parliament, http://www.hmso.gov.uk/acts/acts1998/19980029.htm
[10] GRIA, http://www.gria.org
[11] WS-I Basic Security Profile 1.0, http://www.ws-i.org/Profiles/BasicSecurityProfile-1.0-2004-05-12.html
[12] CorTTex, http://www.corttex.nl/
[13] PARIS, http://www.in4tek.com
[14] Aden T, Eichelberg M, Thoben W, "A fault-tolerant cryptographic protocol for patient record requests", Proceedings of EuroPACS-MIR 2004
[15] ISO 14598-1 (1998) Information technology - Software product evaluation - Part 1: General guide. ISO, Geneva.
[16] WS-Policy, http://www-128.ibm.com/developerworks/library/specification/ws-polfram/
[17] WS-Trust, http://www-106.ibm.com/developerworks/library/specification/ws-trust/