Cookbook for Regional Interoperability Detailed Design Paper #008

Data Access and Consent Management

FOR GENERAL DISTRIBUTION

Version 2.0– 21st December 2019

Abstract Interoperability Cookbook Anchor Points

Section	Title
3.1.3	Consent Server
4.6	Governance for Data Providers

Table of Contents

Version Control

Version	Release Date	Released By	Reason for Release
1.0	20/04/2019	R Hickingbotham	Preliminary Draft
1.1	29/04/2019	R Hickingbotham	Internal Discussion Draft
2.0	21/12/2019	R Hickingbotham	For General Distribution

Reviewers

Initials	Name	Organisation
DM	Dave Maidment	Leeds City Council
GH	George Hope	Leeds City Council
SM	Shaun Smale	LHCR Rapidly Improving Care
TD	Tim Davey	PA Consulting

Release Notes for this Version

1) Expanded on a design for the integration with the National Opt-Out Service

1 Introduction

1.1 Purpose of this Document

This document is one of a series of design papers which underpin the Abstract of a Cookbook for Regional Interoperability (the Abstract Cookbook). These papers, in their totality, describe the technical components and the standards which form the YHCR System of Systems. They are intended as a basis for developing or procuring software and so are expressed at a level of precision which is intended to avoid ambiguity but with a consequence that they are focussed to technical readers.

Design papers are anchored to topics which are discussed in the Abstract Cookbook. They are elaborations of the concepts which were first introduced by the abstract and new content is further detail rather than variations of previously established core principles.

This document (design paper 008 - "Data Access and Consent Management") focuses on mechanisms for controlling policy-based access to data. A large part of this topic relates to consent: the ability for citizens to express their wishes as to how data about them is shared and for the participants in YHCR to systematically enforce these wishes. But policies might be put in place for other reasons, for instance to prevent data being released:

- that is stale or untrusted;
- where there is no current legitimate relationship with the client or patient;
- that is counter to a point-to-point data sharing agreement.

This design establishes boundaries within the YHCR, across which data will not travel, unless it complies with certain rules. The rules are granular and form the basis of policies which specify which data is shared with whom, when and for what purpose. To be applied practically, policies must be enforceable algorithmically. A decision to withhold data, particularly where there is no legal basis to share, cannot be a subjective. One of the key challenges for this design paper is to enable policies to be interpretable to both those subscribing to them and to software which behaves consistently across the YHCR.

1.2 The Relevance of Consent to the YCHR

General Data Protection Regulation (GDPR) requires a legal basis for processing data. A legal basis may be that explicit consent has been obtained by the person to which the data relates. Another is that use is for the purpose of direct care. The YHCR is not required to and will not collect patient consent for the use of their data for direct care.

However, this does not nullify the need for consent management in the YHCR. The YHCR will be used for functions other than direct care which might include, research, risk profiling, service planning, and engagement with relatives or carers. All data may not be strictly necessary for direct care, or for care of a particular nature. Data will also be contributed by the patient's themselves and they may do so on the basis of being able to express consent for its usage.

GDPR is relatively new and is likely to be tested through case law. The YHCR must be able to adapt to any nuances that emerge. Whilst, consent processing may be only be used in a simplistic manner

initially, the presence of a well-considered approach to enforcement will allow future use cases to be onboarded and offer assurance that governance issues will not derail adoption.

1.3 Consent at Source v. Regional Consent Management

One, well established, mechanism for managing consent is for the data controller to capture consent and, only if it is provided, release data to a data processor. This model is problematic for the YHCR:

- consent to process relevant data is not needed for direct care and so restrictions on release may be inappropriate;
- the approach requires citizens to provide consent with every data provider, placing an onus on the citizen to achieve a uniform expression of wishes;
- typically, the expression of consent is a binary share or don't share, whereas the possible uses of data by consumers of the YHCR are diverse.

This paper proposes a different system:

- Citizens wishes are captured locally but held and applied centrally.
- Data controllers release data to the YHCR with the understanding that consent wishes will be applied by the YHCR and some data may be withheld from data consumers.

This approach is compatible with local control over consent. Individual data providers can operate consent rules which supplement regionally managed rules. Indeed, if local control is undertaken in a way which is consistent with regional control, then it is possible to present consent rules to the citizen in an interpretable and consistent manner.

1.4 Policies, FHIR and Consent Management

Consent management is often considered in terms of policies. In this context a policy is something that a citizen can opt into and is a human interpretable statement of what data can be shared and under what circumstances. More generally a policy may control release of data for any reason.

HL7 FHIR offers support for policy-based consent management through its *Consent* resource. The *Consent* resource can be used in a number of different ways but broadly it describes a patient's acceptance of a policy under a set of conditions. What constitutes the policy (which is a uniform, definition of data coverage and circumstances in which they will be shared) and what constitutes conditions (which are an expression of an individual's terms for accepting a policy) is ambiguous.

At STU3 FHIR allows individual conditions to override a policy in a number of areas:

- the purpose for using the data;
- the data items covered;
- the groups, organisations, practitioners, teams, or related people covered;
- the groups, organisations, practitioners, teams, or related people exempted;

R4 further extends the level of personalisation of the policy which is possible.

The ability to record conditional acceptance of a policy is powerful but adds complexity for individuals accepting or rejecting policies, user interfaces on which policy decisions are recorded, and on agents enforcing the policy. Conditional acceptance is particularly problematic for regional enforcement as many of the overrides are defined using references to locally understood concepts.

This paper adopts the following principles:

Policy:	A statement of what data items can or cannot be shared with whom in a particular circumstance.
Consent Resource:	A citizen's acceptance of one or more policies.

These definitions allow standard policies to be defined regionally and applied uniformly across localities. Consent is unconditional: in subscribing to a policy a citizen agrees to its scope in its entirety.

1.5 Relationship of this Document with Other Standards

The following standards form the basis for this document:

- FHIR Release 3 (STU) – Messaging Using FHIR Resources;

1.6 Intended Users of the This Document

This document is a reference guide for data providers implementing a FHIR Proxy Server with consent management features, developers of regional infrastructure, and developers of user interfaces which capture expressions of consent.

2 Modelling Policies and Consent

2.1 Policies

A policy is both:

1. A human interpretable explanation of a situation in which data may be shared or otherwise processed. It covers the reason for processing, the scope of data involved and identifies the organisations or occupational roles of people who will have access to the data.
2. A machine interpretable set of rules which enables computer programs to determine whether data is within the scope of the policy and whether the policy allows it to be released to a data consumer.

A citizen can opt in to a policy which then permits the data which it covers to be used for purposes, and by the organisations/ people, that it states.

Policies are a regional dataset that is maintained by the YHCR. Policies might also be defined and maintained locally. This design is primarily focused on regionally modelled policies but there are clear benefits to having a consistent approach to policy modelling both locally and regionally and this design will be used to guide the development of consent management functionality in the model FHIR Proxy Server (design paper 003).

Policy rules must be actionable and defined in a way that definite determination can be made as to whether data being requested by a data consumer is covered by the policy. Policy rules must define:

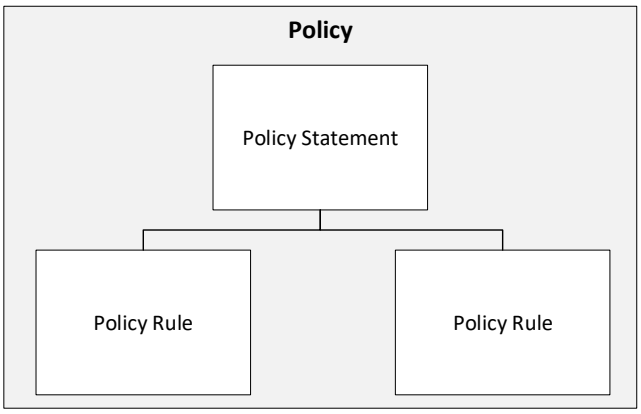
- the context in which the policy describes the data being used (where, by whom, and for what reason);
- the data points which are covered by the policy.

A simple narrative of the policy might require multiple rules to allow it to be implemented. For instance, a policy statement might read:

"I permit my anxiety levels as recorded by me on the XYZ app to be read by my current care team and my nominated carers".

As the care team and nominated carers will be accessing the YHCR with different roles then this policy would need to be implemented as two separate rules: one applying to access by Clinical Professionals and the other for access by Citizens.

A high-level model for a policy is:



The Policy Statement supplies the human readable narrative and some control data whilst the Policy Rules allow machine interpretation of the policy.

2.1.1 Policy Statement

The policy statement contains header fields which apply to the policy as a whole. It includes:

- a policy name;
- human readable narrative describing the policy;
- an optional start date from when the policy comes into force;
- an optional end date from when the policy is retired;
- a basis being inclusive or exclusive;
- a rank which enables an order of precedence to be followed to resolve conflicting policies;
- a scope being individual or global.

The following definitions apply:

Basis

Inclusive: the policy allows data which matches a policy rule to be released. Policies for the purpose of consent must be inclusive – a person must explicitly opt-into a policy for it to have weight as a legal basis for sharing.

Exclusive: the policy restricts release of data which matches a policy rule.

Scope

Individual: the policy can be opted into by a citizen and it is enforced for patient identifiable data.

Global: the policy applies to all data, patient identifiable and otherwise. If installed at a boundary then all data crossing the boundary is released subject to the policy rules.

2.1.2 Policy Rules

A policy rule has three components:

1. Context.
2. Data Coverage.
3. Action.

2.1.2.1 Context

Context represents the data usage to which the data policy applies. It specifies details of who will be using the data, for what purpose, where they will be accessing data from. To be computationally applicable there must be a close correlation between the definition of context and the information provided in an authorisation claim made by a data consumer when accessing the YHCR. Details of the claim are provided by design paper 005 – “Identity and access Management”. Data items which are relevant to the definition of context include:

Claim Field	Explanation	Corresponding Policy Rule Property
iss	The application which issues the claim.	access.from
ods	The ODS code of the organisation that issued the claim.	access.organisation
rsn	The reason for the access request.	access.reason

usr.rol	The user's role.	user.role
usr.org	The ODS code of the organisation who employs the user in the capacity for which they are accessing the YHCR.	user.organisation
usr.rel	The user's relationship with the patient.	user.relationship

Note that v1.0 of design paper 005 – "Identity and Access Management" omitted to define usr.rel. This has been corrected in future versions of the paper.

2.1.2.2 Data Coverage

Data coverage defines the data items that can be released to a data consumer within the context in which the request is being made. It is defined in terms of resource types and search paths. Given an instance of a resource it is possible to execute a search using the search path that allows an enforcer to determine whether a resource is within or outside of the scope of the policy.

The approach to using search paths, rather than resource references (as implemented by the FHIR *Consent* resource), allows the policy to be applied to any patient. An example of a search path for an *Appointment* is:

```
date=gt2013-01-14
```

The interpretation of which is "details of all appointments dated after 1 April 2014 can be released according to this policy".

Data coverage is expressed as an array of data items each referencing a resource definition and textual search path.

Data Item	Explanation
data[n].resource	A reference to a resource definition.
data[n].searchPath	The search path which defines whither the applies.

The array is interpreted so that a resource instance which is matched by any of rules is within the coverage of the policy.

Practical Scope of Using Search Paths to Define Data Coverage

Using search terms to define data coverage is simple but has limitations. Data can be only defined in terms of the properties of the data item itself or data items which are referenced by the base resource.

This allows for defining restrictions such as:

- test results by the location of the encounter in which they were captured;
- prescriptions by the role of the prescribing practitioner;
- care plans by the type of the care team that will action them;
- appointments by the reason for which they were made;
- any data item by its source data provider.

There are many possibilities but there are also limitations, for instance, constraints which are dependent on the presence of another resource. I.e.:

- observation from an encounter in which a particular condition was observed.

All limitations could be addressed by extending the syntax for expressing data coverage. At this stage, in the absence of any policies to model, it is asserted that simple search paths will suffice, and any constraints will be addressed as they are encountered.

2.1.2.3 Action.

The action defines what happens if data is deemed out of coverage of an active policy by an enforcement agent. Options include:

- withhold data without acknowledging the data's existence;
- withhold the data by acknowledge the data types which have been withheld;
- include data but warn that it is breach of the policy.

Section 3 details the mechanism by which the data consumer is notified in the last two of these options.

2.1.3 Policy Data Model

Policies are modelled as resources using a document-based data model. Whilst these are not FHIR resources they can be lodged in a document database and can be managed using the syntax of the FHIR API. The following resource definition reflects the narrative above:

Name	Flags	Card.	Type	Description & Constraints
Policy	I		DomainResource	
identifier	Σ	0..1	Idenitifier	
status	?! Σ	1..1	code	active | inactive
name	Σ	1..1	string	
narrative	Σ	1..1	string	
start	Σ	0..1	dateTime	
end	Σ	0..1	dateTime	
type	Σ	1..1	code	global | individual
rule	Σ	1..*		
access		0..1		
from		0..1	Reference(DataConsumer)	
organisation		0..1	Reference(Organisation)	
reason		0..1	code	Ref. design paper 005
user		0..1		
role		0..1	code	Ref. design paper 005
organisation		0..1	Reference(Organisation)	
relationship		0..1	code	Ref. design paper 005
data		1..*		
resource		1..1	Reference(StructureDefiniotion)	
searchPath		1..*	string	

Search parameters comprise:

Name	Type	Description	Expression
end	date	The end data of the policy	Policy.end
name	string	The name of the policy	Polic.name
identifier	token	The unique id for a particular Policy	Policy.identifier

rule-context-from	reference	Policy contexts targeting a data consumer.	Policy.rule.access.from (DataConsumer)
rule-context-organisation	reference	Policy contexts targeting an organisation	Policy.rule.access.organisation (Organisation)
rule-context-organisation	token	Policy contexts targeting a reason for access	Policy.rule.access.reason
rule-context-userRole	token	Policy contexts targeting a user role.	Policy.rule.user.role
rule-context-userOrganisation	reference	Policy contexts targeting a user organisation.	Policy.rule.user.organisation (Organisation)
rule-context-userRelationship	token	Policy contexts targeting a user relationship.	Policy.rule.user.relationship
status	token	The status of the Policy	Policy.status
start	date	The start date of the Policy	Policy.start

2.2 Consent

Consent is a formal record of a citizen's opt-in to a policy. Consent is modelled regionally and within the YCHR FHIR Proxy Server as FHIR *Consent* resources. The YHCR FHIR Consent resource is a constrained STU3 resource.

The only use of the resource in the YHCR is to record a citizen opt-in and the constraints described here focus on removing the ability to modify the policy through additional conditions. The YHCR profile only applies to regional usage and to those organisations implementing local consent management using the model FHIR Proxy Server.

Element	Resource Cardinality	Profile Cardinality	Implementation Notes
policy	0..1	1..1	A consent resource must use a policy for its scope definition
policy.uri	0..1	1..1	The URI will be a reference to a YHCR Policy resource.
actor	0..*	0..0	The policy context cannot be modified through the resource.
action	0..*	1..1	Action must be 'use'.
securityLabel	0..1	0..0	The policy context cannot be modified through the resource.
purpose	0..1	0..0	The policy context cannot be modified through the resource.
data	0..1	0..0	The policy rules cannot be modified through the resource.
except	0..1	0..0	The policy context and rules cannot be modified through the resource.

2.3 Management of Regionally Held Policies and Expressions of Consent

Regional *Policy* and *Consent* resources are maintained in the Regional FHIR Store (design paper 018). Standard FHIR APIs are used to create and modify the resources. The API is secured using the bearer token mechanism described for the Identity and Access Management Service in design paper 005. As with all regionally held data, the end user must have a regional identity and a regionally assigned

role to manage resources in the regional FHIR Store. The roles required to manage policies and consent are published in the YHCR Operations Guide.

2.3.1 User Interfaces for Recording Consent

The YHCR will not offer a user interface for care professionals to manage their clients/patients consent resources. There are a number of user interfaces across the region which will be interacting with the YHCR and it is anticipated that a number of them will develop consent management functionality over time.

Consent may also be managed directly by the citizen. The Helm person held record is the LHCREs strategic option for a patient and consent self-management functionality is on the roadmap for this product.

3 Policy Enforcement

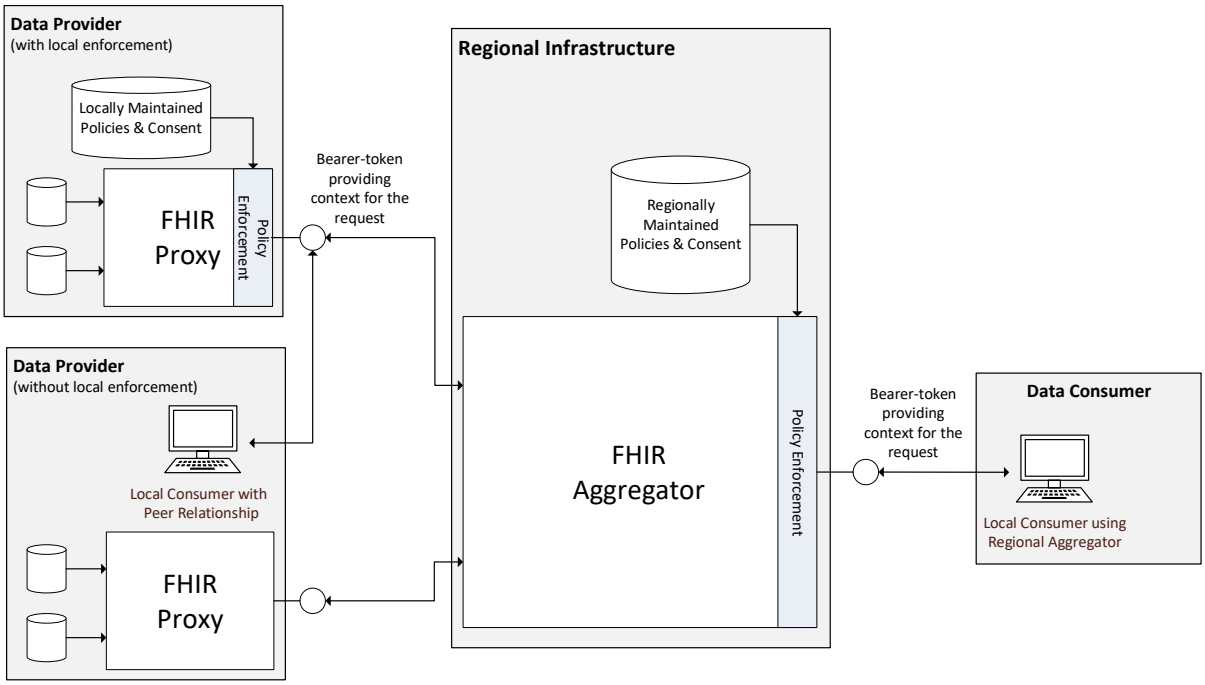
Policies are enforced by the YHCR at boundaries where data passes from data providers to data consumers. The boundary of primary importance for most data consumers is the YHCR Regional FHIR Aggregator Service (design paper 010). The Aggregator will apply policy rules to data received from data providers and will withhold data that does not comply with a policy or for which consent is required and no opt-in received.

A local provider may optionally operate an enforcement boundary and will do so if it:

- has local policies which are not enforced regionally;
- permits access to data from one or more privileged data consumers which bypass the regional Aggregator.

Both regional and local enforcement is enabled by the bearer-token based security infrastructure (design paper 005 – "Identity and Access Management") which provides visibility of an end-users claim to data and provides their context for access.

The enforcement model is depicted as follows:



3.1 When is Consent Enforced?

The enforcement of consent is tied to the reason for access claimed by the data consumer. Until a more nuanced interpretation of direct care emerges following rules will apply:

Code	Reason	Consent Enforced
1.1	Direct care (Emergency). Access is in the context of a patient;	No
1.2	Direct care (Non-emergency). Access is in the context of a patient.	No
2	Indirect care with the consent of the patient. Access is in the context of the patient.	Yes

3	Indirect care not in the context of a patient. (Not patient-centric).	Yes
4	Analytics with access restricted to pseudonymised data. (Not patient-centric).	Yes
5	Administration (Not patient-centric).	N/a

The reasons for access are taken from design paper 005 – "Identity and Access Management"

3.2 Breaking the Glass

Breaking the glass is concept supported by most consent enforcement agents. It relates to a care professional overriding consent rules in exceptional circumstances. It typically involves the care professional making a declaration of why they require privileged access to data, this being logged, and, as a consequence, normal consent processing is circumvented. As GDPR stands, there is no need for break the glass functionality in the YHCR as any emergency access is by definition for the purpose of direct care.

Were the situation to change then the YHCR could accommodate the concept by policies being written which distinguish between reasons for access Direct care (Emergency) and Direct care (Non-emergency).

3.3 Informing Consumers About Withheld and Restricted Resources

A policy action allows for situations where a consumer is informed about which resources are withheld or warned about restrictions relating to resources which are provided.

FHIR bundles allow for meta-data to be embedded in search results using an *OperationOutcome* structure.

If a resource is withheld because of a policy and the policy requires the consumer to be informed that the resource was withheld then the search bundle will contain an entry with no resource but with an *OperationOutcome* structure completed as follows:

severity: information

code: suppressed.

Only one entry will be included for each withheld resource type.

If a resource is included but because of a policy its use is restricted, then the search bundle will include the resource in an entry with an *OperationOutcome* structure completed as follows:

severity: information

code: informational

details: MSG_RESTRICTED_RESOURCE.

4 Relationship with the National Opt-Out Service

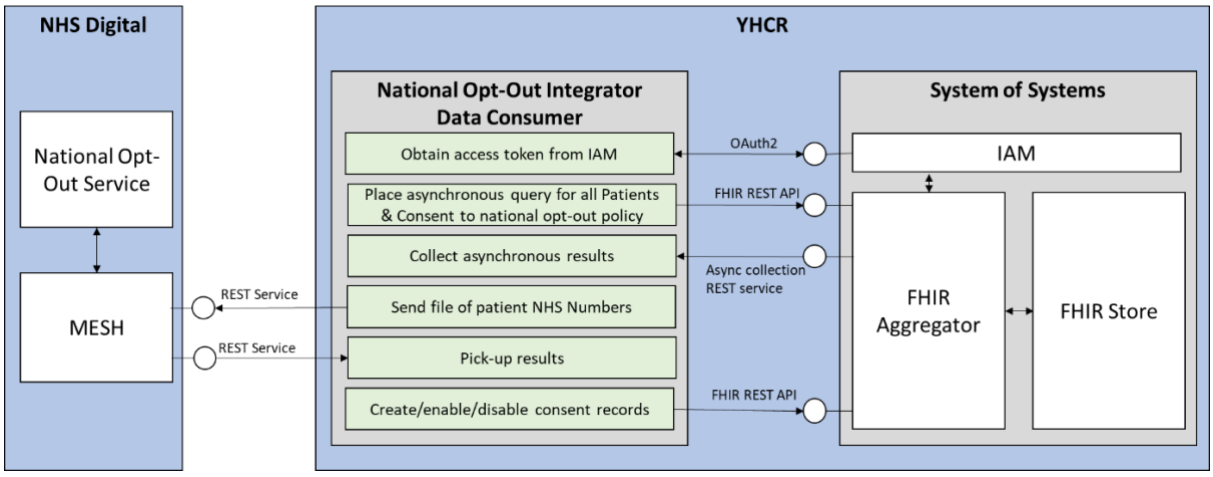
The YHCR is required to comply with the National Opt-Out programme by March 2020. The programme enables patients to opt out from the use of their data for research or planning purposes.

The YHCR will use the consent management infrastructure described in this paper to comply as follows:

1. A policy will be written that denies access to data when the context's 'reason for access' is 4: "Analytics with access restricted to pseudonymised data". The policy will operate on an 'Exclusive' basis and will therefore stop data flowing for this type of access if a consent record exists.
2. Consent resources will be written opting-out of the policy for NHS numbers known to the YHCR (see design paper 004 – "Patient Identity Exchange (PIX/MPI)") where the patients have opted-out at a national level. The use of an Exclusive policy and the reversal of the opt-out/opt-in interpretation means that Consent records will be managed for the YHCR for relatively few patients.
3. The National Opt-out service will be periodically polled by sending a file of NHS numbers over MESH (refer to the service's technical design).
4. The results will be processed, and *Consent* resources will be enabled or disabled accordingly.

4.1 National Opt-Out Integrator as a Client of the System of Systems

The functions described above will be performed by a software product which operates as a client of the System-Of-Systems. The software will be registered with the System-of-Systems as a data consumer and will interact with regional data using standard System-of-Systems APIs. The consumer's interactions are depicted below.



The national Opt-Out integrator will be located on regional infrastructure. It will be executed periodically according to schedule which is published in the Operations Guide. The periodicity will be less than the 7 days mandated by NHS England for retaining opt-out data.

Logically the processing steps are:

1. Obtain a YHCR access token by making a claim against the YHCR Identity and Access Management service (design paper 005). The claim should identify the user's role as 4 : "System or Robot".

2. Query the System of Systems for all patients which are registered with the system of systems. The query need only to obtain NHS numbers and so the content of the result set can be limited to identifiers. The query should be issued asynchronously and so the client is responsible for polling for results.
3. Query the System-of-Systems for Consent resources which are linked to the policy which represents a national opt-out. Again, the query should be executed asynchronously.
4. Prepare a file of NHS numbers in the format mandated by the national opt-out service and dispatch it using the MESH REST service.
5. On receipt of the response file (which contains NHS Numbers for patients which are not opted-out) determine changes required to the Consent resources held by the YHCR.
6. Post/Patch the new/modified consent resources to the System-of-Systems.

Note that the logical processing flow include asynchronous steps and the software will be written to be re-entrant i.e.: to be re-executed to process the results of a previously issued asynchronous instruction.

Appendix 1 – Maturity Matrix

Section	Narrative	Consultative	Draft	Normative
1 Introduction 1.1 Purpose of this Document	X			
1.2 The Relevance of Consent to the YCHR	X			
1.3 Consent at Source v. Regional Consent Management			X	
1.4 Policies, FHIR and Consent Management			X	
1.5 Relationship of this Document with Other Standards	X			
1.6 Intended Users of the This Document	X			
2 Modelling Policies and Consent 2.1 Policies 2.1.1 Policy Statement			X	
2.1.2 Policy Rules			X	
2.1.3 Policy Data Model			X	
2.2 Consent			X	
2.3 Management of Regionally Held Policies and Expressions of Consent 2.3.1 User Interfaces for Recording Consent				X
3 Policy Enforcement 3.1 When is Consent Enforced?				X
3.2 Breaking the Glass	X			
3.3 Informing Consumers About Withheld and Restricted Resources			X	
4 Relationship with the National Opt-Out Programme 4.1 The National Opt-Out Integrator as a Client of the System of Systems			X	