

ACADEMY OF MEDICAL ROYAL COLLEGES

Document Information

Document Acronym	MIPS
Document Title	Medical Interoperability Portfolio Standards (MIPS) Specification Draft Version 0.5
Document Information	This document has been developed as one of the deliverables of the Academy of Medical Royal College electronic portfolio interoperability standards project.
URL	http://www.mips.org.uk/

Document History

Editor	Version	Created	Status	Description
C. Koiak	0.1	10-Sept-10	Draft	Initial version
C. Koiak	0.2	15-Sept-10	Draft	Includes draft entity diagram, LEAP 2A representations and security model (OAuth). Circulated to working group.
A. Lamb, C. Koiak	0.3	27-Sept-10	Draft	New document structure and MIPS classes.
A. Lamb, C. Koiak	0.4	01-Oct-10	Draft	Incorporates working group feedback.
A.Lamb	0.5	02-Oct-10	Draft	Review of all sections
C. Koiak	0.6	15-Dec-10	Draft	Added MDC on every entry; replaced supporting information type with Leap2A types; Added commentary support to SI.

Contributors

Name	Role	Organisation
Andrew Lamb	Web Services Director	Royal College of Surgeons of Edinburgh
Simon Grant	Technical Consultant	JISC CETIS
Chris Koiak	Technical Architect	Conscia
Iain Moir	Project Manager	Conscia
Mark Buchner	Managing Director	Conscia
Edgar Steenvoorden	Consultant	DH Interoperability Working Group
Chris Bell	Consultant	DH Interoperability Working Group
Tim Jackson	Consultant	Premier IT

In addition much of the ideas for the basis of this specification have evolved from discussions and contributions from the AoMRC interoperability standards project group and the DH interoperability working group.

Contents

1.	Introduction	6
1.1.	Summary	6
1.1.1.	Overview of Interoperability Standards	6
1.1.2.	The NHS N3 gateway	7
1.2.	Scope	9
1.2.1.	Aims & Scope of Standards	9
1.2.2.	Exclusions from scope	10
1.3.	Scenarios of Practice	10
1.3.1.	General Practice (RCGP Scenario)	11
1.3.2.	NHS Hospital Based Doctor	11
1.3.3.	Private Hospital Based Specialist	13
1.3.4.	GMC Access to Revalidation Information	14
1.4.	MIPS Data Classification (MDC)	14
1.4.2.	Applicability of DH Information Levels	16
1.5.	Licence	16
2.	MIPS Standard 0.9 Draft	17
2.1.	Classes	17
2.1.1.	Base Object	19
2.1.2.	Person	20
2.1.3.	Organisation	21
2.1.4.	Supporting Information	21
2.1.5.	Resources/Files	22
2.1.6.	Context Selection	22
2.1.7.	Supporting Information Extension Attribute	23
2.2.	Types, Categories and Syntax Recommendations	23
2.2.1.	Context Selection Type	24
2.2.2.	Supporting Information Types	24
2.2.3.	Supporting Information Extension Attribute Type	25
2.2.4.	Id Syntax recommendations	26
2.3.	Intersystem Communication	27
2.3.1.	Web Services	27
2.3.2.	Communication Models	28
2.4.	Security	31

2.4.1. System Authentication.....	31
3. Policy	35
3.1. Base object.....	35
3.2. Person	35
3.3. Organisation	36
3.4. Context Selection	37
3.4.1. Appraisal Selection.....	37
3.4.2. Revalidation Selection.....	38
3.4.3. Curriculum Vitae Selection	38
3.4.4. Employment Application.....	38
3.4.5. Clinical Excellence Award Application.....	38
3.4.6. Exam Eligibility Selection.....	38
3.4.7. Course Eligibility Selection	38
3.5. Supporting Information	38
3.5.1. SI – Compliant	39
3.5.2. SI – Significant Event.....	40
3.5.3. SI – Case Review	40
3.5.4. SI – Patient Feedback	41
3.5.5. SI – Colleague Feedback	41
3.5.6. Multi Source Feedback.....	42
3.5.7. SI – Additional Supporting Information.....	42
3.5.8. SI – Other Roles	43
3.5.9. SI – Teamwork.....	43
3.5.10. SI – Health.....	43
3.5.11. SI – Probity	43
3.6. Control Files.....	44
3.6.1. Policy XML.....	44
3.6.2. Provider List.....	45
4. Example Implementation.....	46
4.1. Implementation Process	46
4.2. Leap2A	47
4.2.1. Definition and Suitability	47
4.2.2. Class mappings.....	48
4.2.3. Leap2A Examples	48
5. N3 Gateway.....	53

5.1. Background.....	53
5.2. Description of the N3 gateway.....	54
5.3. Delivery, maintenance and future upgrading.....	55
5.4. Deliverables.....	56
5.4.1. Gateway Administration & Policy Manager.....	56
5.4.2. N3 Gateway Provider System.....	57
5.4.3. MIPS Consumer demonstration implementation.....	58

1. Introduction

1.1. Summary

This document outlines the standards that should be adhered to for successful interoperability between professional medical portfolio information systems. The standard is an open source standard that can be used by any number of systems. The standard has been designed to have the flexibility to be adapted to support future medical revalidation and professional development requirements. The document then goes on to discuss an example implementation of the standards in the form of an “N3 Gateway” application.

1.1.1. Overview of Interoperability Standards

This standard is a combination of existing standards that have been combined to address the different areas of interoperability

- **Authentication & Security** – All requests for data will be authorised by the user associated with the data. All transferred data will clearly identify the sensitivity of the information contained. OAuth¹ 2.0 standard and MIPS Data Classification will be used to achieve this, both are described in detail later.
- **Data Structure** – MIPS defines a set of classes/entities and categories that can be used to describe portfolio data to be transferred. This architecture provides the flexibility to adapt to new requirements as they evolve. All data will be transferred in LEAP2A² structure. LEAP 2A is an Atom³ based XML document structure that has been developed to describe general portfolio data.
- **Data Messaging** – All data will be requested through REST-based HTTP requests. This will only be used to read data via GET requests; updating and delete information in remote systems is not currently supported by MIPS. REST based web services are prevalent due to their simplicity, flexibility and coherence with web based requests.

These combined open standards provide a comprehensive architecture for securely and consistently transferring electronic portfolio information between systems.

¹ <http://en.wikipedia.org/wiki/Oauth>

² <http://www.leapspecs.org/2A/>

³ http://en.wikipedia.org/wiki/Atom_%28standard%29

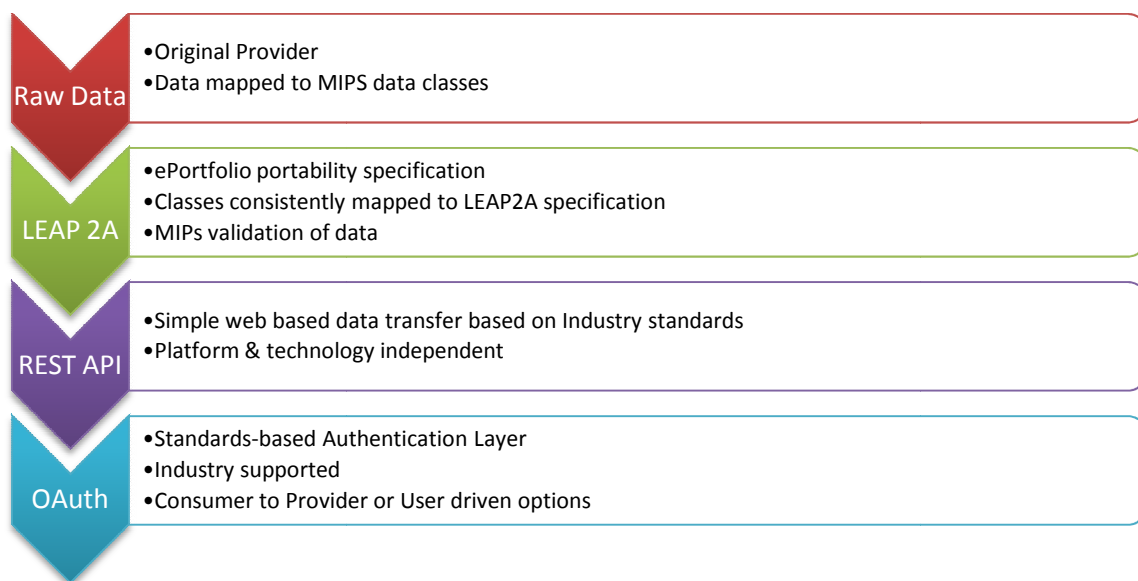


Figure 1: Standards-based communication layers

This document then proceeds to discuss an implementation of this standard that would support data transfer in and out of the NHS secure network (N3) and should result in an understanding of the construction of the ‘N3 Gateway’ solution.

1.1.2. The NHS N3 gateway

The N3 gateway project sets out to demonstrate a “proof of concept”. It is designed around the consideration that much of the information which a doctor needs to supply as supporting evidence for their portfolio, is held within the confines of the NHS N3 network and within the data governance jurisdiction of a local trust environment. This information will require collection and storage, but will only be accessed in a detailed fashion on occasion, however important summary (and non sensitive) information can be drawn from this supporting information and be made available without compromising either local or national data governance rules. The N3 gateway aims to provide an N3 compliant solution to the problem which allows a user to aggregate locally sensitive information and transfer to 3rd party portfolio systems only non sensitive information according to the defined MIPS interoperability standards.

Exemplar:-

Thus the typical process of handling such data through the gateway would be, for example, collection of supporting information related to a complaint; this might include; a letter from Patient, a response from the Trust, an account of the event by the doctor, a response to the

patient by the trust, summary of outcome, etc.

In order for the effective assessment of the event, it is necessary for this information to be available securely for reference, however at this stage there is no particular reason for this detailed information to leave the organisation. It is necessary though to record some information about the complaint episode; i.e. when did it happen, how long did it take to come to resolution, the doctor's summary of the complaint, what was the outcome, if the doctor has changed their practice subsequently, etc. This information is important to be readily available for the doctor's portfolio and arguably does not compromise sensitive information (except about the individual doctor). If, subsequently, access is required to the full information it is important that the information is aggregated and accessible via an N3 compliant and locally governed mechanism without the subsequent need for further manipulation of the data. It is crucial therefore that the information is pre-prepared for ready access but also transition from the N3 environment to external scrutiny, if required by the appraisal process. The unpredictable timing of when patient sensitive information will be required to leave the confines of the local environment for external evaluation, or any other reason, makes the conditions for storage of this data such that they are compliant with the standards dictated by statute at outset.

Therefore the model of the gateway is as follows:

- To provide a locally controlled repository of supporting information that the doctor can upload all information that they feel is relevant to gain a full understanding of the event. This is securely retained within the repository and access to this is controlled by the local authority.
- To be able to answer some standard questions about the event, the answers to which are then available to be drawn down by one or more externally based portfolios to become part of the doctor's portfolio record. The questions asked will be defined by the policy section of these interoperability standards, although the design allows these to be overridden by local policy if needs be.
- To provide information to external portfolios on how the detailed supporting information can be accessed in the situation where further information is to be sought. This information is likely to be in the form of a unique identification number identifying the event, together with information about where the full event information is held i.e. Trust, Local Authority or National System. Access to the full (potentially containing patient

sensitive information) event information then remains governed by the local authority via local mechanisms.

The full specification of the N3 gateway is included at the end of this document, and is intended principally to provide a practical demonstration of the implementation of the standards.

1.2. Scope

It is important to describe the scope of the standards including what they are trying to achieve and what is outside of the scope of the standards.

1.2.1. Aims & Scope of Standards

The standards aim to provide a set of precise rules that allows medical portfolios to either request and receive data or send data in a format that will allow both the transmitting and receiving systems to attribute the same or very similar meaning to the portfolio content, thus achieving a greater level of integration than simply the transfer of unstructured files.

Through the leveraging of existing standards, aim to achieve as high a level of interoperability with existing educational based portfolio systems thus opening the opportunity for as wide a choice of possible of systems integration.

To provide an extensible set of standards that will cope with the information requirements now and into the future as the nature and requirements of medical portfolios evolve.

To propose a model of how systems will interact with each other including a proposal on how Organisations, systems and People will be identified within the portfolio system space. This includes; a master List of Organisation identities, recommendations for Organisation ID Syntax, System ID Syntax, and Person ID Syntax.

The standard defines a simple set of basic classes that when arranged together can represent portfolio data components and how they might be linked together. In addition the standard defines an Initial Dictionary of attributes applicable for extending the basic supporting information classes to support the revalidation templates. This Class model therefore together with the dictionaries provides a basis for how portfolio data will need to be transformed before transmission.

In the Policy area of the standards there is defined an initial set of evidence (supporting) information types which are constructed as a result of discussions and consensus during the lifetime of this project. However we envisage that this area of the standards will evolve as portfolio data requirements become more defined. To this end the standards have been designed to support the evolution of these policies.

Security and Data governance are extremely important when considering medical portfolios. This standard proposes a data classification to assist in the handling of portfolio data (MIPS Data Classification or MDC). This proposes 4 possible categories one of which can be applied to each of the attributes and attachments associated with supporting information types based on Policy templates. This approach goes some way to assisting in the automated handling of data both in terms of security prerequisites and data governance issues. This classification is also cross matched against the eGif classification for security for data objects transmitted, which helps to define the infrastructural security requirements.

1.2.2. Exclusions from scope

This standard does not dictate the internal data structure of existing or future portfolio systems; it simply specifies the format and structure that portfolio data items need to be translated into in order to be consistently transmitted.

The standard also does not specify the structure and content of individual supporting information items, but provides a flexible approach that supports existing supporting information structures to be adapted and new structures to be added.

The Policies section provides some recommended base supporting information templates that can be used for revalidation together with recommended classifications of the data items in terms of security and data governance sensitivities (MDC levels), however these are purely template recommendations and as long as the dictionary classifications are adhered to these templates can be overridden or changed completely to support different or new supporting information types.

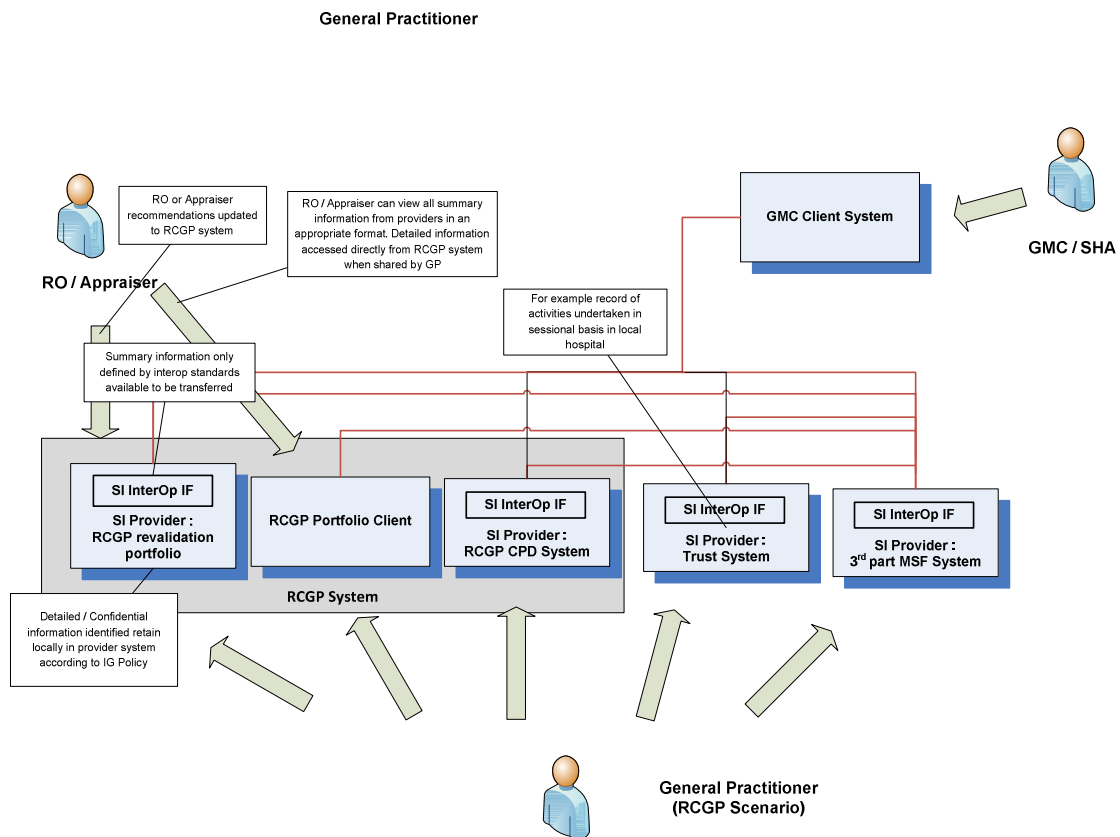
1.3. Scenarios of Practice

This section presents a non exhaustive list of scenarios that these interoperability standards are designed to support. Each presents similar but differing interoperability challenges and have

required careful consideration in terms of data governance and security considerations.

1.3.1. General Practice (RCGP Scenario)

In the General Practice revalidation scenario the General Practitioner will generally keep their supporting information evidence directly within the RCGP system with the Appraisers and revalidation officers also members of the system and having full access to the supporting evidence information when the needs require. The main areas of interoperability requirements come from external providers of information such as third party course or learning systems (such as doctors.net, BMJ eLearning). There is potential a need for interoperability from N3 based systems where a GP undertakes part of their work in a trust environment (i.e on a sessional basis).



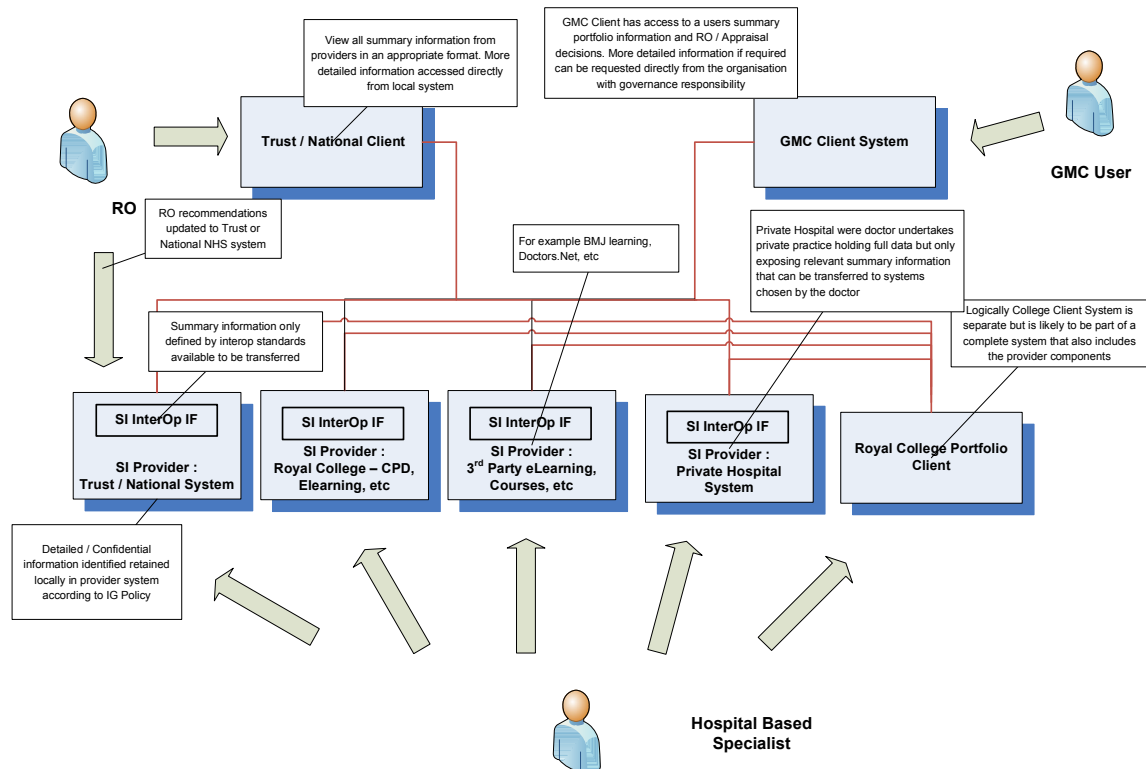
1.3.2. NHS Hospital Based Doctor

Revalidating doctors working in hospital often will be principally based in one trust where the appraiser and revalidation officer will also work. In this situation all parties will likely have access

to the same system and thus the interoperability requirements will be similar to the scenario for General Practitioners. There are many situations however where re hospital based doctors workload many be split either between trusts, private practice and or academic commitments. In this situation there is a requirement for interoperability between systems, often involving data of a sensitive nature if clinically based.

1.3.2.1. Notes on scenario

- Doctor principally working in a single trust
- Revalidating Doctor and RO or Appraiser will normally be using the same trust system so access to detailed information (MDC 4) in this circumstance not an issue
- MDC 1,2 & 3 information held in other systems by doctor will be immediately available to RO & Appraiser through trust based system, if revalidation doctor provides information about the information provider and delegates access.
- MDC 4 information held in other systems i.e. other trusts, private hospitals requires information governance agreements between organisations.

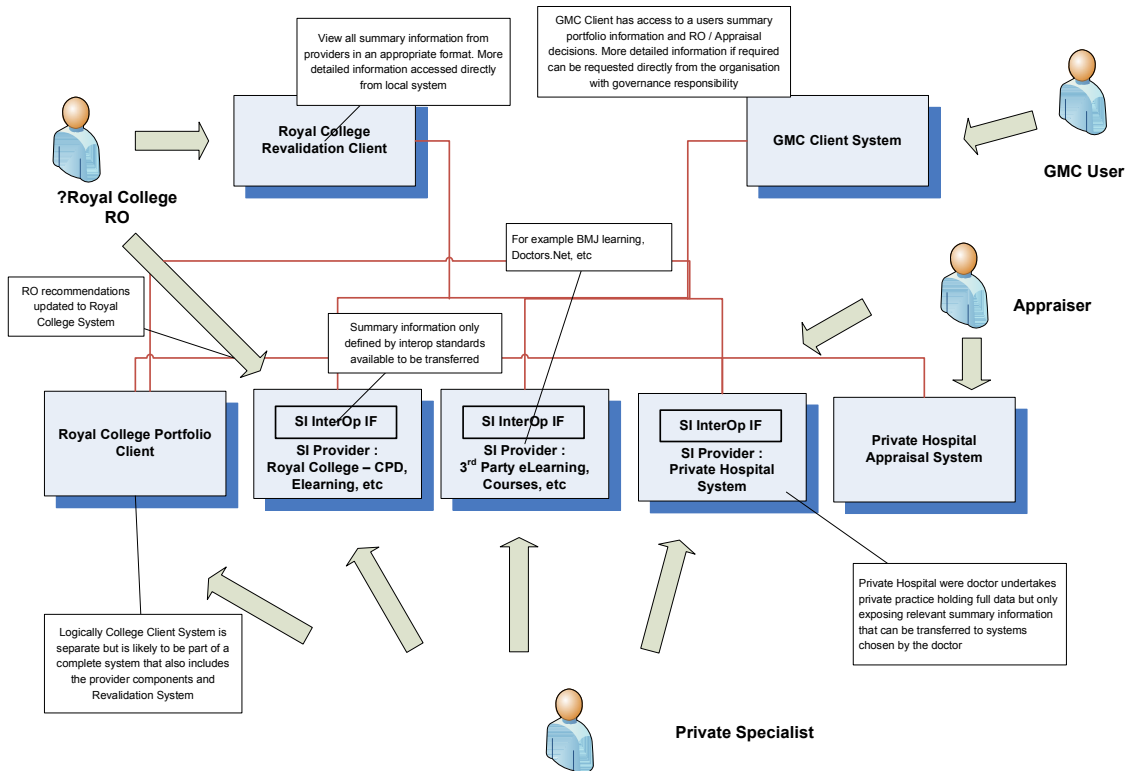


1.3.3. Private Hospital Based Specialist

If a doctor is principally based in a private hospital environment, the scenario is very similar to the NHS based hospital where the Appraiser and Revalidation Officer will likely utilise the same revalidation system and thus have locally controlled full access to the appraises relevant records. The situation becomes more complex however if the doctor also undertakes work outside the private hospital environment and there is a need for interoperability with external systems.

1.3.3.1. Notes

- Appraisal potentially undertaken in Private Hospital.
- Professional supporting information potentially held in a number of systems
- RO will have access to MDC 1,2 & 3 information directly by revalidating doctor providing access
- Access to MDC 4 information by RO will require information governance agreements between organisations.



1.3.4. GMC Access to Revalidation Information

It is unclear at the time of writing these standards, the exact nature of the interoperability requirements of Appraisal and revalidation systems and the UK General Medical Council. However we would anticipate at the very least there would be a requirement to be able to electronically request or receive a record of a revalidation recommendation. It may also be desirable for a request to be possible for MDC 1,2 and 3 categories of information used as supporting information for the revalidation Appraisals, in the situation where a doctor's revalidation recommendation requires the GMC to investigate further. We would therefore anticipate that with the Appraisees consent, that this level of interoperability would be supported by the standards.

1.3.4.1. Notes

- GMC system could access MDC 1,2,3 information if revalidating user has shared this or the data item is the revalidation decision.

1.4. MIPS Data Classification (MDC)

In considering the scenarios requiring interoperability, it became clear that there was a need for a simple and understandable classification to be applied to data items of a portfolio which will be applicable both for data within an NHS environment and also in commercial situations. The classification of items informs the system of how it should handle data in terms of what can and cannot be transferred out of the system and in terms of what type of security should be applied – according to local security and data governance policies. Four basic types of data have therefore been defined.

1.4.1.1. MDC Category 1

This is principally descriptor data that notes the occurrence of an activity, usually including its date. Importantly disclosure of this information would not cause the professional any significant reputational harm. Please note however that these standards do not play any role in dictating the policy of what should or should not be transferred from an organisation, the policies are purely recommendations which may or may not be adopted by the host provider system.

1.4.1.2. MDC Category 2

This information will generally include qualitative structured information about the activity either created by the professional or a co worker about the activity. Examples of this might be “What I have learnt from this complaint”, “What I plan to do differently”, “How patients rated your communications skills”. Disclosure of this information could cause reputational harm to the professional, however should not cause reputational harm to any co-worker or patient.

1.4.1.3. MDC Category 3

This will generally be raw unstructured data which importantly has been certified by an individual as being anonymised. It therefore can cause reputational harm to the professional but not to any patient or co-worker. Its principal use is to provide extended data which can provide background information for an assessment process but which with the permission of the professional generally could be transferred out of the source organisation. Importantly MDC Category 4 information may be subsequently converted into MDC Category 3 data by a standardised process, particularly if there is a subsequent request for more information about an event from an external authority.

1.4.1.4. MDC Category 4

This kind of data will generally be unstructured raw data which may or may not contain patient identity information and or information about co-workers. It potentially therefore can cause reputational harm to the professional and to a patient or co-worker. Its principal use is to provide extended data which can provide background information for an assessment process but where an individual seeking access will have to be granted access through local data governance procedures. Generally local policy will dictate that this sort of information should never be transferred from the organisation.

The table below provides an overview of the classification.

MDC Level	Description	Owner is the Person Record is About	DH IL	Colleague Identifiers
MDC 1	Descriptor Data	Yes	2	No
MDC 2	Qualitative Data	Yes	3	No
MDC 3	Anonymised Data	Not Necessarily	3	No
MDC 4	Raw Data	Not necessarily	3	Maybe

MDC Level	Contains Patient	Tamper Evident	Authored by	Authored by some other
-----------	------------------	----------------	-------------	------------------------

	Identifiable Information (PII)		professional	named person or body
MDC 1	No by definition	Yes	Usually	Possibly
MDC 2	No (certified anonymous)	no	usually	Possibly
MDC 3	No (certified anonymous)	no	Possibly	Possibly
MDC 4	maybe	Yes	Possibly	Possibly

1.4.2. Applicability of DH Information Levels

The DH information levels consider the security that should be applied to different types of data transferred in terms of their potential reputational harm if the security is breached. We would consider that most portfolio data should be considered IL3 with the possible exception of MDC 1 data.

1.5. Licence

Please see www.mips.org.uk/licence/.

2. MIPS Standard 0.9 Draft

The Medical Interoperability Portfolio Standards (MIPS) provide a consistent method for representing and communicating users' electronic medical portfolio information. Using this standard protocol, information may be transferred out of systems acting as portfolio *providers* and imported into systems acting as *consumers*; Consumer systems may be established ePortfolio systems, Provider systems may be other ePortfolio systems or any information system that holds medical portfolio related information about a doctor.

Every element of information to be transferred can be classified by the MIPS Data Classification (MDC) to identify how it has been treated from a security and data governance viewpoint in the originating host system. The policy part of this document gives recommendations as to how different types of data should be classified, however it is up to the host system to implement the security systems and impose the policies on the data items. The classification can however be applied in a default manner by using the standard policy elements within this standard.

The classes (data elements), method of transfer and authentication mechanism are defined in this standard.

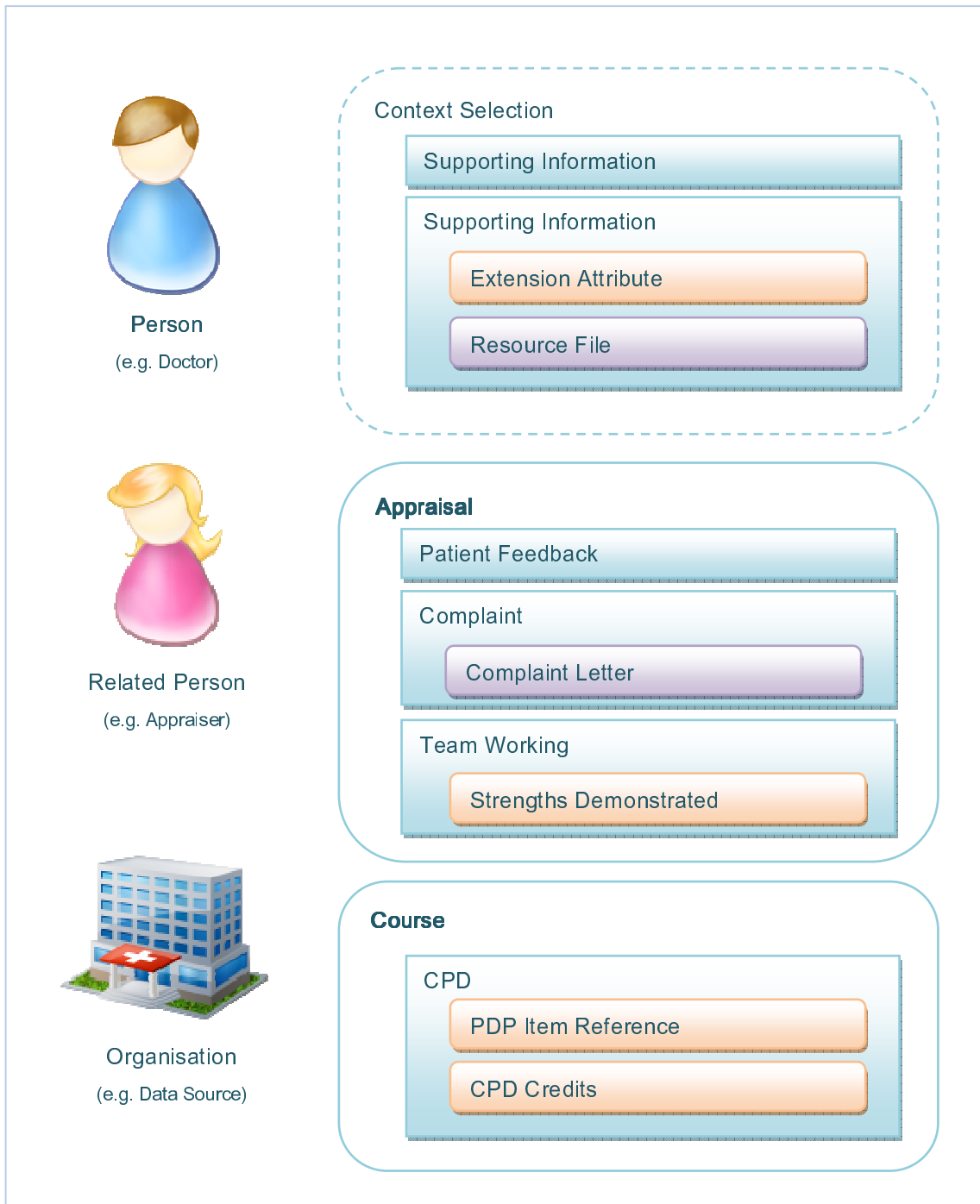
2.1. Classes

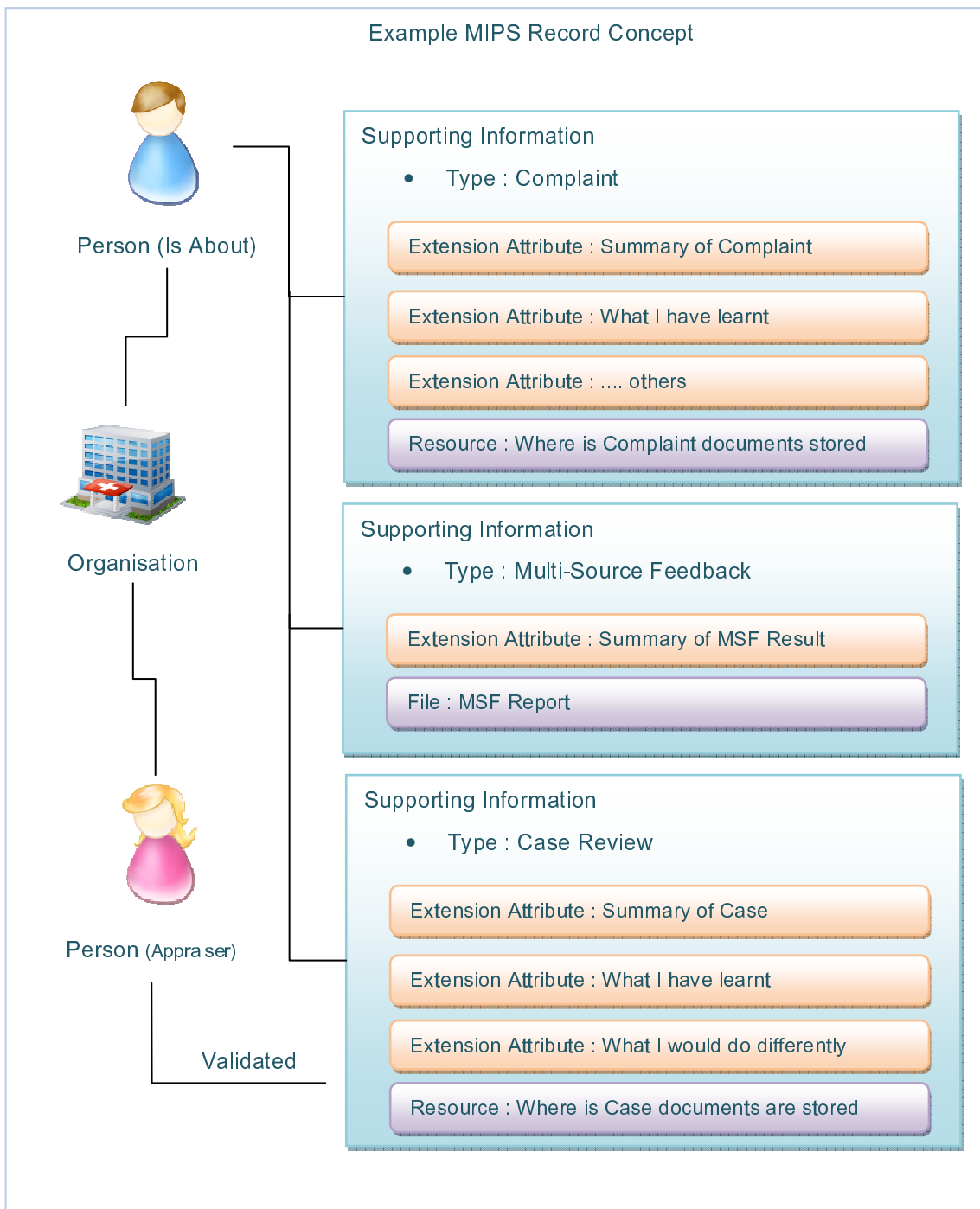
The MIPS classes have been defined to be as generic as possible in order to provide flexibility and future proofing. They consist of a number of base data elements that together form the foundations of the portfolio data entities, on top of these a number of generic data items are added to build up the complex data structures required to represent the composite portfolio data entities. This is deliberately a high level definition of system elements to provide the most flexibility during implementation. Thus in this model complex pieces of supporting or other information relating to a doctor are assembled as many small generic parts following a basic pattern described here.

The MIPS policy section defines the recommendation for extension attributes and their applicable MDC classifications for some common types of portfolio supporting information thought to be relevant to revalidation and appraisal.

It is intended that validation systems will be developed to both validate MIPS messages and also optional their adherence to specific policy templates. Thus as the understanding of the

revalidation requirements evolve and consolidate, the ability to enforce rules through the standards can potentially also evolve.





2.1.1. Base Object

The base object defines the basic information class which all other classes are based on.

Every element **MUST** contain

- Identification that gives the item uniqueness in a universal sense – i.e. this will usually be the originating system URI together with the originating system identification of the element (e.g. www.doctors.net/SI/ID12345)
- Creation date
- Originating System Identification, this can be assumed to be inherited from a parent object if not specified.
- Data Governor Organisation, this can be assumed to be inherited from a parent object if not specified.
- MIPS Data Classification (MDC) of the object. Although this is primarily intended for Supporting Information it must appear on all data objects for consistency.

Every element SHOULD

- Link to the Person it is about, even indirectly, unless it is the pertinent person element itself.

Every element should describe all its relationships, including those that are described in parent elements. For example, a parent element (Supporting Information) must describe all child elements (Extension Attributes) and all child attributes must describe all parent relationships. This allows the context of any element to be determined from itself, without the need to evaluate all elements.

2.1.2. Person

The person element defines an individual that is related in some way (either the information is about them or they have a role in the information i.e. appraiser) to one or more pieces of data being transferred. Any information that is transferred MUST include at least one person class which represents the person that the information is about.

Besides information required for the base object, each person element MUST contain

- One or more identifiers for this person (for example GMC number, IMC number or Employer Reference Number) , examples include www.gmc-uk.org/ID/123456, www.sometruster.nhs.gov.uk/ID/123456 .
- The person's context within the data set – They may be the primary doctor, an appraiser, etc.
- Forename
- Surname

- Title

A person MAY be linked to

- Supporting Information
- Groupings of Information

2.1.3. Organisation

The organisation element defines an organisation that is related to one or more pieces of data being transferred.

Besides information required for the base object, each organisation element MUST contain

- Name of the organisation
- Organisation Unique Identifier examples include www.sometruster.nhs.gov.uk, www.doctors.net, www.bmj.com

Each organisation element MAY contain

- Contact telephone number
- Contact address

2.1.4. Supporting Information

A supporting information element is the documentation of a significant event related to the user's portfolio. In these standards the supporting information concept is extended to include any information that may be of relevance to a user in respect of their portfolio.

Besides information required for the base object, each Supporting Information element MUST contain

- Title – A descriptive title of the type of Supporting Information, this may add more context than the Type alone would provide.
- Type of information – from the Supporting Information Type vocabulary (e.g. Patient Complaint, Patient Feedback, Appraisal Outcome, Details of General Practitioner)
- Valid date – A nominal date for the purposes of searching that relates to a point in time that this item is valid. Note however that a descriptive version of this may be included for display purposes i.e. “spring 2007”
- Summary of information

Supporting Information SHOULD have

- Validated By – If available, a person who has validated this supporting information
- Validated On – If available the date a person validated this information.

Supporting Information MAY have

- Link to one Context Selection
- Links to one or more Supporting Information Extension Attributes
- Links to one or more Resources or files

2.1.5. Resources/Files

A resource element defines an electronic or physical document or file that contains relevant information. This may be a file or resource that is included in the transmission or it may be a reference to a file or resource which is not included. The file or resource may not be included for a number of reasons such as the owning organisation may not wish this resource to be transmitted for data governance reasons, or the resource may be felt to be too large in size to be transmitted.

Each Resource element must contain

- The type of resource
- An URI OR a description of how to obtain the document
- Link to the Supporting Information it relates to

2.1.6. Context Selection

The Context Selection element groups supporting information into a context. For example this may group some supporting information that relates to an appraisal, an exam application or job application.

Each Context Selection element MUST contain

- Title
- Type – from the Context Selection Type vocabulary
- Target date
- Links to one or more Supporting Information elements

Each Context Selection element MAY contain

- Applicable Location
- A status – i.e. pending submission

2.1.7. Supporting Information Extension Attribute

Extension attributes represent the bulk of the actual portfolio data to be transferred. The available types are defined in the extension attribute type vocabulary. In this version of standards those felt to be most important for revalidation have been included, however it is anticipated that this vocabulary will be extended in future versions. Extension attributes are principally used to extend the Supporting Information objects to hold information relevant to the activity. The extension attributes that should be used to extend a supporting information object for a particular supporting information type are recommended in the policy section of this document (supporting information templates).

Each Extension Attribute element MUST contain

- A Title – A descriptive title of the attribute. It may be the original question that was asked to gather the attributes value.
- Type – from the Extension Attribute Type vocabulary
- Content – The value of the attribute
- Link to the Supporting Information related to this attribute.

Each Extension Attribute element MAY contain

- A value enumeration – in the case of an integer value this attribute may contain a list of value meanings (e.g. 1 = Always, 2 = Sometimes, etc)

2.2. Types, Categories and Syntax Recommendations

The standard contains three defined vocabularies for cataloguing

- Context Selection (Grouping) Types
 - E.g. Appraisal selection, Revalidation Selection, CV Selection, Job Application Selection
- Supporting Information Types
 - E.g. MSF, Patient Feedback, Patient Complaint, Elogbook Report, Appraisal Result
- Extension Attribute Categories

- “Summary of Complaint”, What I have Learnt, What I plan to do differently in the future”

This is understood to be the most volatile section of the standard, as it is likely to evolve as areas of revalidation become better defined.

In addition the Syntax of various descriptors is recommended these include

- an Organisation ID Syntax,
- a System ID Syntax,
- a Person ID Syntax

2.2.1. Context Selection Type

The valid Context Selection types are

- Appraisal Submission
- Revalidation Submission
- CV Selection
- Employment Application
- Merit Award Selection
- Exam Eligibility Selection
- Course Eligibility Selection
- TBC

2.2.2. Supporting Information Types

The valid Supporting Information types are

- Significant Event
- Case Review
- Patient Feedback
- Colleague Feedback
- Additional Supporting Information
- Other Roles
- Teamwork
- Health
- Complaint
- Probity

- Appraisal Result
- Revalidation Result
- GMC Recommendation
- Multi Source Feedback
- Operative Logbook Report
- Audit Report
- Outcomes Report
- Other Supporting Information

2.2.3. Supporting Information Extension Attribute Type

The standards group recognises that there is significant work underway developing a matrix of common appraisal attributes and are awaiting the outcome of this work before consolidating this section.

The valid Extension Attribute types defined are

- What went well
- What could have been done better
- Learning & Development
- GMP Mapping (Value will have the actual mapping details)
- Related Speciality
- Validated Date
- Validated By
- CPD Credits
- PDP Item Reference
- General Reflection
- Summary of Complaint
- TBD: This list needs to be complete

2.2.4. Commentary Type

- Review
- Reflection
- Approval

2.2.5. Id Syntax recommendations

The recommendation for the syntax of Ids is where ever possible to use URI based identification possibly with a URL and sub address.

Examples

An Organisation ID

www.sometruster.nhs.gov.uk

A System ID

www.sometruster.nhs.gov.uk/Systems/ID12345

A person ID

www.gmc-uk.org/list/123456

N.B. It is desirable that these URLs are real and could return confirmatory or extended information about the identity, however this is not a necessity.

2.2.5.1. Person ID Syntax

A Person may have multiple Ids, the primary Id is the originating systems ID for the Person. The mostly commonly used global identifiers are GMC or IMC identifiers, which we would recommend would be in the following format: www.gmc-uk.org/list/123456 or www.medicalcouncil.ie/list/123456 .

2.2.5.2. Extension Attribute Syntax

All extension attributes ids should extend the format of the object they relate to by applying a suffix to the related object's id.

systemId:objectType/uniqueId/attributeName

2.3. Intersystem Communication

All communication will be based on web services. Read only operations are supported at this time, update or delete requests are not supported.

Each provider MUST define their own URI for their web service, for example <https://www.example.com/portfolio> or <https://example.com/a/b/c>

All data passed between systems should be regarded as transient. It is recommended that a provider should not disseminate data it has gathered from another provider.

If data is disseminated from a non-originating system then the data must be clearly identified and must respect the original MIPS Data Classifications and Ids of each element.

Providers MUST return Leap2A compliant XML – tools to assist developers in validating these systems will be made available through the MIPS site in due course.

Providers SHOULD provide a minimal level of information for each piece of data they hold. For example, if a system holds MDC 4 data but isn't including it in the data export, it should include MDC 2 entries and indicate that more information is available. Within the feed, this should be represented as a link element to the further information, which could be represented as a resource or organisation.

2.3.1. Web Services

Two web services must be available to return

- Person Data
- File Data

The Person Data web service must accept the following parameters.

- MIPS Data Classification
- Person Identifier
- Applicable date range – Start and End dates
- Supporting Information MDC category – Optional – if used then data at or below that level will only be returned – i.e. this can be used by passing MDC 1 to return just summary descriptive information.

The File Data web service must accept the following parameters

- File Identifier

2.3.1.1. Person Data

This standard recommends that the person data web service is implemented as RESTful web service.

The structure of this REST web service would be

[baseURI]/[MDC]/[PersonID] /[start date]/[end date]/[SI Type]

The Supporting Information type is an optional attribute.

For example, <https://www.eportfolio.com/mips/4/www.gmc-uk.org%2Flist%2F1234567/2010-10-01/2010-10-31/complaints> would return all information for GMC number 1234567 that is valid for October 2010 relating to the Complaints type. (Note the gmc domain in the person ID has been URL encoded)

2.3.1.2. File Data

This standard recommends that the file data web service is implemented as RESTful web service.

The structure of this REST web service would be

[baseURI]/[MDC]/file/[fileid]

For example, <https://www.eportfolio.com/mips/4/file/7854> would return the electronic document identified by the eportfolio as 7854.

2.3.2. Communication Models

There is no technology restrictions on how the MIPS specification should be implemented, as

long as the system implements the standards then it can communicate with any other compliant system.

The MIPS standard is designed to initially support peer to peer communication; however it could in the future be extended with a set of Hubs that relay communication.

2.3.2.1. Peer to Peer

Peer to Peer communication means that each Consumer system will communicate directly with the Provider system.

The majority of implementations will utilise the Peer to Peer model; where Consumer systems communicate directly with Providers. Some systems may be both a Provider and Consumer.

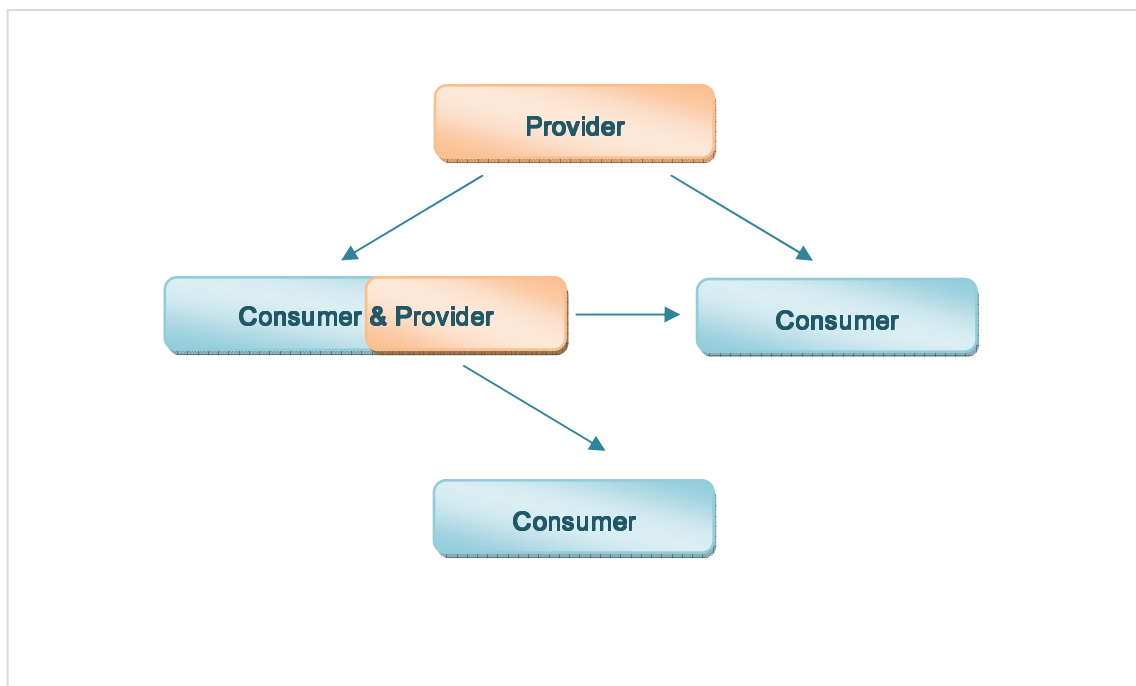


Figure 2: Peer to Peer model

2.3.2.2. Hub Architecture

All systems must have an externally visible URL to allow system communication. In some cases this may not be possible, for example a system may wish to communicate with a system inside a private network (N3).

The communication specification could be extended to allow communication to go through a Hub. This hub would be dual-homed across the internal and external networks where it could relay messages.

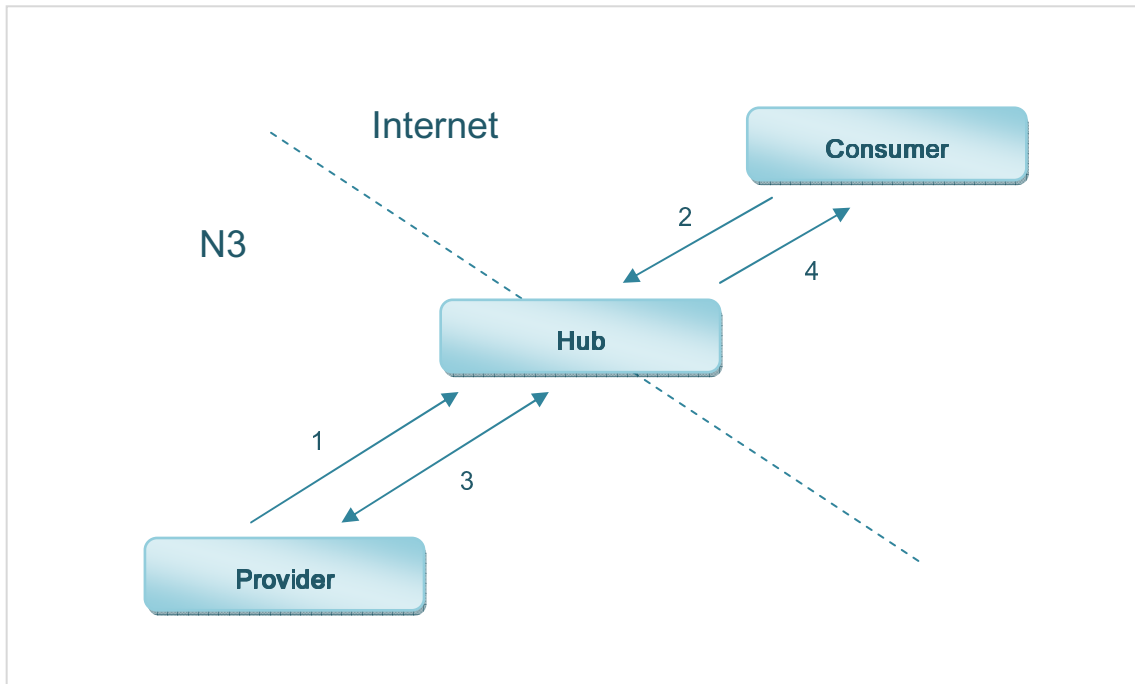


Figure 3: Hub Architecture

In the above example the Provider resides on N3 and information is required by a Consumer. (1) The provider would open a listening connection to Hub and wait for a request. (2) The Consumer would make all requests the Hub rather than the Provider, where the hub would call the Provider (3) for the request. This would finally be returned to the Consumer (4) as if it came directly from the Provider.

The Hub could apply additional policies to the data being transferred. An example of an additional policy may be to not allow any MDC 4 or MDC 3 Complaint information outside of the network (N3).

A centralised Hub could also support full audit logging. It would need to be centrally managed and could result in a communication bottleneck.

2.4. Security

2.4.1. System Authentication

This specification recommends the use of OAuth for authorisation and access control between systems. In adherence with OAuth, all data **MUST** be transferred across HTTPS.

All requests for data from a Provider shall only be accepted from a known, trusted and validated Consumer. All consumers must register with each provider that they wish to retrieve data from, each provider will issue a consumer key and secret.

Access to a user's data on the provider system must be authorised by the user before any data is transferred.

2.4.1.1. OAuth

OAuth is an open protocol that supports authorization and API access delegation between web applications. It began development in 2006 by Twitter, with Google supporting in the creating of the OAuth 1.0 specification. The Internet Engineering Task Force (IETF) published the OAuth 1.0 as RFC 5849⁴ in April 2008. OAuth is regarded⁵ as the combined wisdom of propriety industry protocols such as Google AuthSub⁶, Yahoo BB Auth⁷ and Flickr API⁸

OAuth extends the established client-server authentication model and incorporates the third role of resource owner. In order for the client (consumer in MIPS) to gain access to the server (provider in MIPS) the resource owner must grant permission. This is achieved by the consumer redirecting the owner to the provider system, where they authorise the request and are then returned to the consumer system. This is know as 3-legged OAuth and is the traditional implementation.

MIPS Provider and consumer systems **MUST** support 3-legged OAuth.

⁴ <http://tools.ietf.org/html/rfc5849>

⁵ <http://hueniverse.com/oauth/guide/intro/>

⁶ <http://code.google.com/apis/accounts/docs/AuthForWebApps.html>

⁷ <http://developer.yahoo.com/auth/>

⁸ <http://www.flickr.com/services/api/>

The provider should not put a time limit on how long a consumer can have access; however the accounts should be disabled as required.

Code libraries exist to ease implementation of OAuth including DefDefined⁹

The diagram below outlines the authentication message flow between a provider and consumer system.

⁹ <http://code.google.com/p/devdefined-tools/wiki/OAuth>

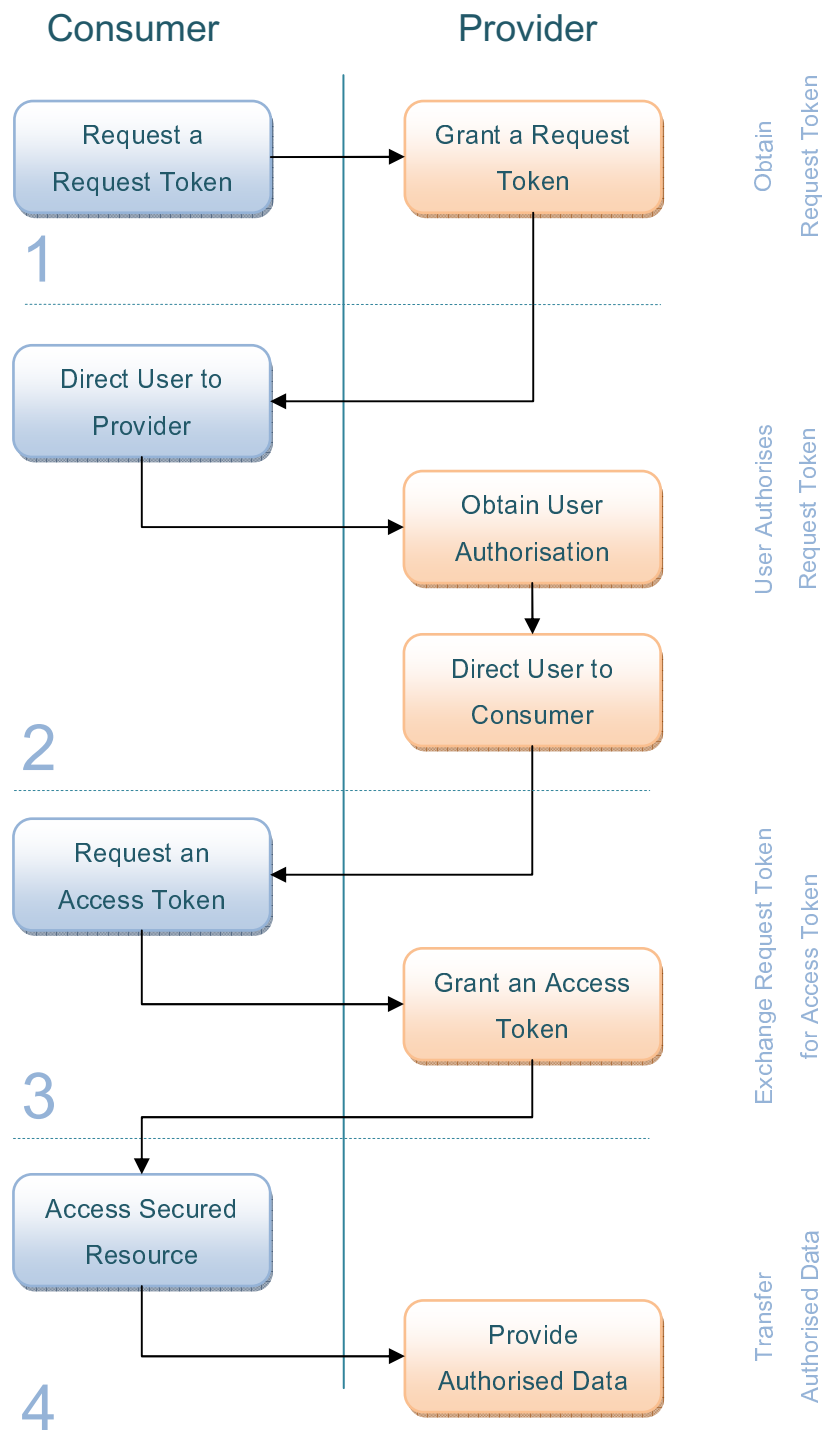


Figure 4: OAuth Authentication Flow

Stage 2 above involves the user being passed to the provider system to confirm that the

consumer is allowed to retrieve their data. Therefore the authorisation that the consumer can access the user's resources is firmly between the user and the providing system. The user would be presented with a screen similar to the one below.

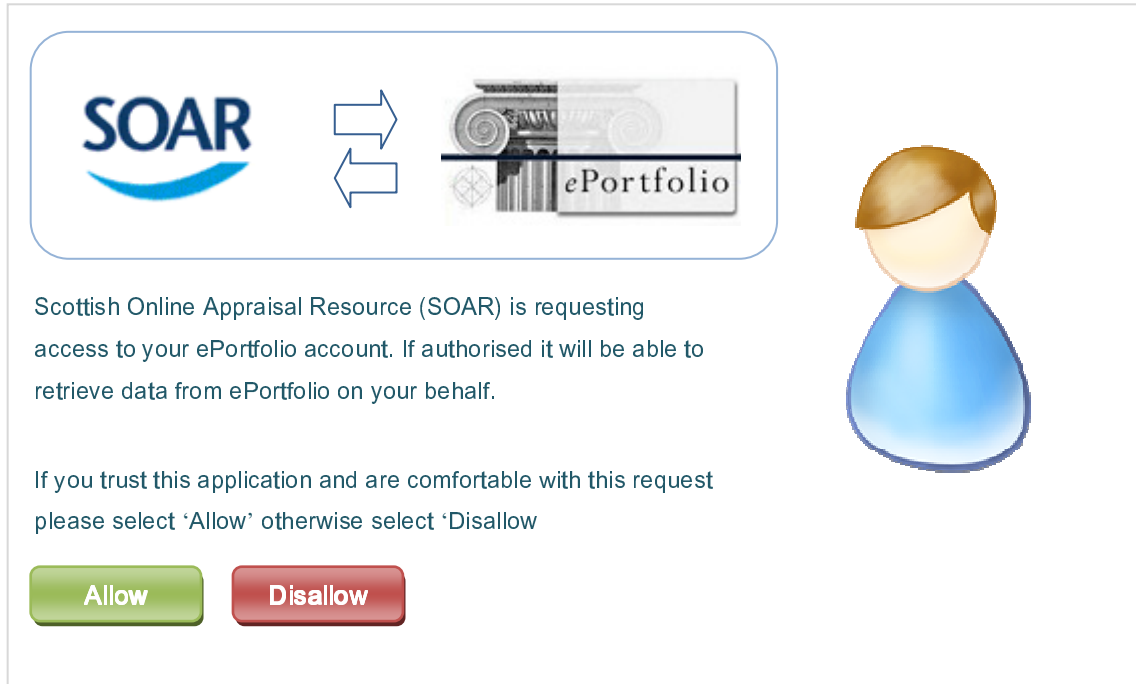


Figure 5: OAuth Authorisation Screen

The user will only have to grant authorisation for a consuming system once. The consumer system will then use this Access Token every time it requests information from the provider.

3. Policy

The MIPS Policy outlines what attributes SHOULD be transferred for each supporting information or context selection. It details the attributes that are mandatory for each type and the MDC of each attribute.

3.1. Base object

The base object is not a policy item however has been included in policy to indicate the recommended MIPS Data Classification Categories for the base object.

Attribute	Mandatory	MDC	Type	Leap2A
Id	Yes	1	String	atom:id
Created Date	Yes	1	Date	atom:updated
Originating System Id	Yes	1	Relationship	atom:link rel="mips:creator" href=" leap2:organisation"
Data Governor Id	Yes	1	Relationship	atom:link rel="mips:data_governor" href=" leap2:organisation"
MDC	Yes	1	String	category scheme="mips:mdc"

The Originating System and Data Governor may be specified under the feed element in the XML feed if they are applicable to all elements. Individual elements can override this as required.

The primary feed element should contain an indication of the highest classification of data contained within the feed.

Should the originating system be represented as the 'Author', the only issue is that a name must be specified (uri should be specified)? If above approach is taken, we need to define mips:creator and mips:data_governor in the standards.

Do we need both an originating system and data governor?

3.2. Person

Person class is included in policy principally for the recommended MIPS Data Classification

Categories.

The Person class should be represented in Leap2A as leap2:person.

Attribute	Mandatory	MDC	Type	Leap2A
GMC Number	No	1	String	leap2:persondata field="id" service="www.gmc-uk.org/list"
IMC Number	No	1	String	leap2:persondata field="id" service="www.medicalcouncil.ie/list"
Type	Yes	1	String	leap2:Person_Type
Forename	Yes	2	String	Combined in the atom:title field in format "Surname, Forename, Title"
Surname	Yes	2	String	As above
Title	Yes	2	String	As above
Supporting Information	No	N/A	Relationship	atom:link rel="leap2:supported_by"
Context Selection	No	N/A	Relationship	atom:link rel="leap2:supported_by"

Need example of Person where originating system is specified and where it's assumed from the feeds id

3.3. Organisation

Organisation class is included in policy principally for the recommended MIPS Data Classification Categories.

The Person class should be represented in Leap2A as leap2:organisation.

Attribute	Mandatory	MDC	Type	Leap2A
Name	Yes	1	Date	atom:title
Telephone Number	No	2	String	leap2:orgdata field="workphone"
Address	No	2	String	atom:spatial

3.4. Context Selection

All Context Selection elements should adhere to the following policy. Additional policies apply for each Context Selection type.

The Person class should be represented in Leap2A as leap2:selection.

Attribute	Mandatory	MDC	Type	Leap2A
Title	Yes	1	String	atom:title
Target Date	Yes	1	Date	leap2:date point="target"
Type	Yes	1	Type	rdf:type resource="mips:selection_type"
Supporting Information	Yes	1	Relationship	atom:link rel="leap2:supported_by"
Location	No	2	String	atom:spatial
Status	No	2	String	leap2:status

3.4.1. Appraisal Selection

Listed below are the recommendations in this version of the standards for extension attributes to be linked to the Context Selection.

Extension Attribute	Mandatory	MDC	Type	Leap2A
Location	Yes	1	String	atom:spatial
Appraiser	Yes	1	Relationship	atom:link rel="leap2:attended_by"
Medical Indemnity Insurance Validated	No	2	Boolean	atom:link rel="leap2:has_part"
Criminal Charges Exist	No	2	Boolean	atom:link rel="leap2:has_part"
CPD Overview Last Year	No	2	String	atom:link rel="leap2:has_part"
CPD Improvements for next year	No	2	String	atom:link rel="leap2:has_part"
Appriasee Registered with GP	No	2	Boolean	atom:link rel="leap2:has_part"

3.4.2. Revalidation Selection

This policy item will be developed when there is clarity on what additional information should be provided.

3.4.3. Curriculum Vitae Selection

Extension Attribute	Mandatory	MDC	Type	Leap2A
Personal Statement	No	1	String	atom:link rel="leap2:has_part"

3.4.4. Employment Application

Extension Attribute	Mandatory	MDC	Type	Leap2A
Personal Statement	No	1	String	atom:link rel="leap2:has_part"
References	No	2	String	

3.4.5. Clinical Excellence Award Application

Extension Attribute	Mandatory	MDC	Type	Leap2A
Personal Statement	No	1	String	atom:link rel="leap2:has_part"
References	No	2	String	

3.4.6. Exam Eligibility Selection

Extension Attribute	Mandatory	MDC	Type	Leap2A
Personal Statement	No	1	String	atom:link rel="leap2:has_part"
References	No	2	String	

3.4.7. Course Eligibility Selection

Extension Attribute	Mandatory	MDC	Type	Leap2A
Personal Statement	No	1	String	atom:link rel="leap2:has_part"
References	No	2	String	

3.5. Supporting Information

All Supporting Information elements MUST adhere to the following policy. Additional optional policies apply for each Supporting Information category.

The mandatory field only applies if the consumer is requesting the corresponding MDC level. For example, a MDC2 attribute is not mandatory if the consumer requests MDC1 data.

The Supporting Information class should be represented in Leap2A as either leap:activity, leap:meeting, leap:achievement, leap:ability, leap:affiliation, leap:plan, leap:publication or leap:entry. The most suitable Leap2A type should be used. The fact that there is a MIPS SI category will allow MIPS consumers to identify the data correctly.

Attribute	Mandatory	MDC	Type	Leap2A
Valid Date	Yes	1	String	leap2:date point="target"
Title	Yes	1	String	atom:title
Type	Yes	1	Type	rdf:type resource="mips:supporting_information_type"
Description	No	2	String	atom:description

Every piece of Supporting Information can have a commentary of remark, review and validation. These items should be represented as Leap2A entries and use the mips reflection category to indicate if the reflection is a review, reflection or validation.

The following sections contain suggested extended attributes for the basic supporting information object. These “templates” are likely to change and evolve as agreements are made across medicine of the commonalities, there is also likely however to be individual variation of these within medical specialties.

3.5.1. SI – Compliant

Extended Attribute	Mandatory	MDC	Type	Leap2A
Summary of Complaint	Yes	2	String	atom:link rel="leap2:has_part"
What I have Learnt	No	2	String	atom:link rel="leap2:has_part"
How have I changed	No	2	String	atom:link rel="leap2:has_part"

my practice				
Status	No	2	String	atom:link rel="leap2:has_part"

File / Resource	Mandatory	MDC	Type	Leap2A
Link to Anonymised Resource	No	3	String	atom:link rel="leap2:has_evidence"
Anonymised File (e.g. associated correspondence)	No	3	Link	atom:link rel="leap2:has_evidence"
Link to raw resource	No	4	String	atom:link rel="leap2:has_evidence"
File (e.g. original correspondence)	No	4	Link	atom:link rel="leap2:has_evidence"

Note : There may be multiple files or resources linked to one supporting information object

3.5.2. SI – Significant Event

Attribute	Mandatory	Type	MDC
TBC			

File / Resource	Mandatory	MDC	Type	Leap2A
Link to Anonymised Resource	No	3	String	atom:link rel="leap2:has_evidence"
Anonymised File (e.g. associated correspondence)	No	3	Link	atom:link rel="leap2:has_evidence"
Link to raw resource	No	4	String	atom:link rel="leap2:has_evidence"
File (e.g. original correspondence)	No	4	Link	atom:link rel="leap2:has_evidence"

Note : There may be multiple files or resources linked to one supporting information object

3.5.3. SI – Case Review

Attribute	Mandatory	Type	MDC
TBC			

File / Resource	Mandatory	MDC	Type	Leap2A
Link to Anonymised Resource	No	3	String	atom:link rel="leap2:has_evidence"
Anonymised File (e.g. associated correspondence)	No	3	Link	atom:link rel="leap2:has_evidence"
Link to raw resource	No	4	String	atom:link rel="leap2:has_evidence"
File (e.g. original correspondence)	No	4	Link	atom:link rel="leap2:has_evidence"

Note : There may be multiple files or resources linked to one supporting information object

3.5.4. SI – Patient Feedback

Attribute	Mandatory	Type	MDC
TBC			

File / Resource	Mandatory	MDC	Type	Leap2A
Link to Anonymised Resource	No	3	String	atom:link rel="leap2:has_evidence"
Anonymised File (e.g. associated correspondence)	No	3	Link	atom:link rel="leap2:has_evidence"
Link to raw resource	No	4	String	atom:link rel="leap2:has_evidence"
File (e.g. original correspondence)	No	4	Link	atom:link rel="leap2:has_evidence"

Note : There may be multiple files or resources linked to one supporting information object

3.5.5. SI – Colleague Feedback

Attribute	Mandatory	Type	MDC
TBC			

File / Resource	Mandatory	MDC	Type	Leap2A
-----------------	-----------	-----	------	--------

Link to Anonymised Resource	No	3	String	atom:link rel="leap2:has_evidence"
Anonymised File (e.g. associated correspondence)	No	3	Link	atom:link rel="leap2:has_evidence"
Link to raw resource	No	4	String	atom:link rel="leap2:has_evidence"
File (e.g. original correspondence)	No	4	Link	atom:link rel="leap2:has_evidence"

Note : There may be multiple files or resources linked to one supporting information object

3.5.6. Multi Source Feedback

Attribute	Mandatory	Type	MDC
TBC			

File / Resource	Mandatory	MDC	Type	Leap2A
Link to Anonymised Resource	No	3	String	atom:link rel="leap2:has_evidence"
Anonymised File (e.g. associated correspondence)	No	3	Link	atom:link rel="leap2:has_evidence"
Link to raw resource	No	4	String	atom:link rel="leap2:has_evidence"
File (e.g. original correspondence)	No	4	Link	atom:link rel="leap2:has_evidence"

Note : There may be multiple files or resources linked to one supporting information object

3.5.7. SI – Additional Supporting Information

Attribute	Mandatory	Type	MDC
TBC			

File / Resource	Mandatory	MDC	Type	Leap2A
Link to Anonymised	No	3	resource	

Resource				
Anonymised File (e.g. associated correspondence)	No	3	file	
Link to raw resource	No	4	resource	
File (e.g. original correspondence)	No	4	file	

Note : There may be multiple files or resources linked to one supporting information object

3.5.8. SI – Other Roles

TBC

3.5.9. SI – Teamwork

TBC

3.5.10. SI – Health

TBC

3.5.11. SI – Probity

TBC

3.6. Control Files

3.6.1. Policy XML

The policy will be defined in an XML file that can be used to validate the information gathered and transmitted.

This file will be available online and could be used to create input forms for data capture that adhere with MIPS policy.

```
<Policy xmlns="http://www.mips.org.uk">
  <version>http://www.mips.org.uk/2010-10/Policy</version>

  <selection type="appraisal">
    <attribute alias="location" datatype="string" mandatory="true"
mdc="4">Location</attribute>
    <attribute alias="appraiser" datatype="mips:Person" mandatory="true"
mdc="4">Appraiser</attribute>

    <attribute alias="medical_indemnity_insurance_validated" datatype="boolean"
mandatory="false" mdc="3">Medical Indemnity Insurance Validated</attribute>
    <attribute alias="criminal_charges_exist" datatype="boolean" mandatory="false"
mdc="3">Criminal Charges Exist</attribute>
    <attribute alias="cpd_overview_last_year" datatype="string" mandatory="false"
mdc="3">CPD Overview Last Year</attribute>
  </selection>

  <supporting_information type="all">
    <attribute alias="validated_date" datatype="datetime" mandatory="true"
mdc="4">Validated Date</attribute>
    <attribute alias="validated_by" datatype="mips:Person" mandatory="true"
mdc="4">Validated By</attribute>

    <attribute alias="what_went_well" datatype="string" mandatory="true" mdc="3">What
went well</attribute>
    <attribute alias="what_could_have_been_done_better" datatype="string"
mandatory="true" mdc="3">What could have been done better</attribute>
    <attribute alias="learning_development" datatype="string" mandatory="true"
mdc="3">Learning & Development</attribute>

    <attribute alias="domain1_attribute1" datatype="string" mandatory="true"
mdc="3">Domain 1 Attribute 1</attribute>
    <attribute alias="domain4_attribute3" datatype="string" mandatory="true"
mdc="3">Domain 4 Attribute 3</attribute>

    <attribute alias="related_speciality" datatype="string" mandatory="true"
mdc="3">Related Speciality</attribute>
  </supporting_information>

  <supporting_information type="complaint">
    <attribute alias="status" datatype="string" mandatory="false"
mdc="3">Status</attribute>
  </supporting_information>
</Policy>
```

3.6.2. Provider List

All providers participating in the MIPS programme must be defined and identifiable. This allows consumer applications to discover new sources of data as they are available.

Each consumer would still be required to establish validate security keys with each new provider to enable interoperability.

Each entry on the provider list will include the provider's institution, system name and URI. The URI MUST be the location of the MIPS web services, it MAY also be the location of the provider system's user interface.

The provider list URL is <http://www.mips.org.uk/ProviderList/>

3.6.2.1. Example

Please note this is an example of the data structure and should not be regarded as the full list.

```
<providers xmlns="http://www.mips.org.uk">
  <provider
    institution="Royal College Surgeons Edinburgh"
    system="ePortfolio"
    uri="http://www.rcsed.ac.uk/eportfolio"/>
  <provider
    institution="Royal College Surgeons Edinburgh"
    system="Courses"
    uri="http://www.rcsed.ac.uk/courses"/>
  <provider
    institution="NHS Education for Scotland"
    system="SOAR"
    uri="https://online.scottishappraisal.scot.nhs.uk/MIPS"/>
</providers>
```

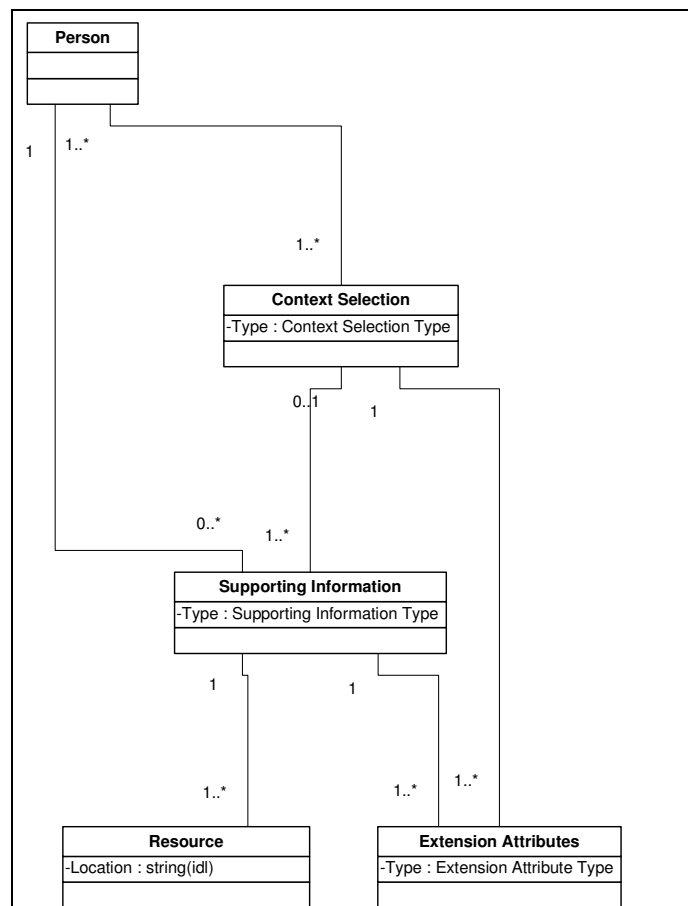
4. Example Implementation

This section will guide a system administrator to identify how to transform their established system to provide or consume data according to the MIPS standard.

4.1. Implementation Process

All systems will represent their data in different data structures using a variety of technologies. However every system can identify the entities and attributes that they use, usually this can be expressed as an UML entity diagram.

The MIPS entity diagram is a simple diagram, when combined with the vocabularies in the Policy, should accommodate most existing systems.



The primary task during implementation is to map the existing system entities to the MIPS structure. For most systems this will mean abstracting their structures to fit the diagram above.

One practical approach would be to list each existing entity in tabular format and assign it to a MIPS class and type. For example an 'Interview' entity may map to a 'Context Selection' of type 'Appraisal'.

After this the mandatory attributes of each MIPS type should be mapped to existing fields. For example the Appraisal type has mandatory attributes for the Location and Appraiser that may exist in the 'Interview' entity as venue and organiser fields.

4.2. Leap2A

4.2.1. Definition and Suitability

Leap2A is a specification "intended to cover the representation of several kinds of information, centred around individuals, who collect, create, reflect on and use their own information for learning, development, self-presentation, or related purposes"¹⁰

The Leap2A specification has a long development history, dating back to 2006. It has been actively developed by CETIS, in conjunction with JISC, from 2007 until the present. It has been adopted by a number of ePortfolio providers and Higher Education institutes.

A Leap2A document is an XML document based on the ATOM standard. All entities derive from the 'Entry' class and are linked to each other using the <link> element. This means that there is no hierarchical structure, but rather a series of multidimensional links.

The Leap2A classes, relationships and categories cover the majority of entities within a portfolio system. However, it is open to interpretation on best use of classes.

The MIPS extends the categories within Leap2A and defines a mapping of Leap2A classes to MIPS classes. No additional classes are specified, MIPS can be viewed as adding a layer of classification on top of Leap2A

As the data is structured in XML it can be extended when required to accommodate new data structures. Furthermore as MIPS is an extension of Leap2A, current Leap2A implementations could consume MIPS data without modification.

¹⁰ http://wiki.leapspecs.org/2A/specification#About_this_specification

4.2.2. Valid Class mappings

MIPS	Leap2A
Person	leap:person
Organisation	leap:organisation
Context Selection	leap:selection, leap:meeting, leap:activity
Supporting Information	leap:activity, leap:meeting, leap:achievement, leap:ability, leap:affiliation, leap:plan, leap:publication, leap:entry
Extension Attribute	atom:entry
Resource	leap:resource

4.2.3. Leap2A Examples

All examples in this document are available for download at <http://www.mips.org.uk/examples>

TBC

As Leap2A is based on the ATOM standard then the output is essentially a list of <entry> elements contained in a <feed> element. Leap2A utilises the <link> element to create relationships between the <entry> elements.

Below is a simple Atom example (without any features of Leap2A or MIPS).

```
<?xml version="1.0" encoding="utf-8"?>
<feed xmlns="http://www.w3.org/2005/Atom">
  <title>Example Feed</title>
  <link href="http://example.org/" />
  <updated>2003-12-13T18:30:02Z</updated>
  <author>
    <name>John Doe</name>
  </author>
  <id>urn:uuid:60a76c80-d399-11d9-b93C-0003939e0af6</id>

  <entry>
    <title>Atom-Powered Robots Run Amok</title>
    <link href="http://example.org/2003/12/13/atom03" />
    <id>urn:uuid:1225c695-cfb8-4ebb-aaaa-80da344efa6a</id>
    <updated>2003-12-13T18:30:02Z</updated>
    <summary>Some text.</summary>
  </entry>
</feed>
```

4.2.3.1. Namespaces

There are a few namespaces required to be included in the feed.

- `xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"`
 - This namespace allows the document to utilise the rdf classes. This is used to apply a 'type' to distinguish each 'entry' element.
- `xmlns:leap2="http://terms.leapspecs.org/"`
 - Supports the usage of all Leap2A classes
- `xmlns:categories="http://wiki.leapspecs.org/2A/categories/"`
 - Supports Leap2A categories that apply further context to each type
- `xmlns:mips="http://www.mips.org.uk/specification/"`
 - The MIPS categories that will be used
- `xmlns:portfolio="http://anysystem.originator.com/"`
 - An identifier of the originating system. This will be used to uniquely identify all elements in CURIE notation.

4.2.3.2. Person Example

```
<feed xmlns="http://www.w3.org/2005/Atom"
  xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
  xmlns:leap2="http://terms.leapspecs.org/"
  xmlns:categories="http://wiki.leapspecs.org/2A/categories/"
  xmlns:portfolio="https://www.northscotlandtrust.nhs.uk/appraisals"
  xmlns:mips="http://www.mips.org.uk/specification/categories">

  <title>MIPS data feed</title>

  <id>https://www.northscotlandtrust.nhs.uk/appraisals/3/https%3A%2F%2Fwww.northscotlandtrust.nhs.
uk%2Fgmc%2F111222%20/2010-01-01/2010-12-31</id>
  <updated>2010-10-08T20:25:05-08:00</updated>

  <!-- The href point to the leap2:organisation element -->
  <link rel="mips:creator" href="http://www.northscotlandtrust.nhs.uk"/>
  <link rel="mips:data_governor" href="http://www.northscotlandtrust.nhs.uk"/>

  <category scheme="mips:mdc" term="3"/>

  <entry>
    <title>Smith, John, Dr</title>
    <id>https://www.northscotlandtrust.nhs.uk/gmc/111222</id>
    <updated>2010-01-12T11:03:55Z</updated>
    <leap2:persondata leap2:field="id" leap2:service="www.gmc-uk.org/list/">
      111222
    </leap2:persondata>
    <rdf:type rdf:resource="leap2:person"/>
    <category scheme="categories:person_type#" term="Self"/>
    <category scheme="mips:mdc" term="1"/>
    <link rel="leap2:supported_by" href="portfolio:appraisal/3242"/>
    <!--
      Optional declaration of the creator and data governing organisation
      N.B. This are redundant in this example as they only repeat the feed links
    -->
    <link rel="mips:creator" href="http://www.northscotlandtrust.nhs.uk"/>
    <link rel="mips:data_governor" href="http://www.northscotlandtrust.nhs.uk"/>
  </entry>

</feed>
```

4.2.3.3. Organisation Example

```
<entry>
  <title>NHS North Scotland</title>
  <id>http://www.northscotlandtrust.nhs.uk</id>
  <updated>2010-01-12T11:03:55Z</updated>
  <leap2:orgdata leap2:field="workphone">
    0123 456 7890
  </leap2:orgdata>
  <rdf:type rdf:resource="leap2:organization"/>
  <category scheme="mips:mdc" term="1"/>
  <spatial>123 Main St, Inverness, Scotland</spatial>
</entry>
```

4.2.3.4. Context Selection Example

This example uses the MIPS Context Selection Type of Appraisal Submission.

SG – “category scheme syntax needs discussion and clarification, in conjunction with supplying a category scheme page. Probably easiest to have a separate category element for each term, but need to check this with Atom and Leap2A.”

Are the category terms allowed to have spaces? Is it more suitable to replace them with underscores?

```
<entry>
  <title>Appraisal Interview</title>
  <id>portfolio:appraisal/3242</id>
  <updated>2010-09-15T11:03:55Z</updated>
  <rdf:type rdf:resource="leap2:selection"/>
  <leap2:date leap2:point="target">2011-03-01T10:00:00Z</leap2:date>
  <category scheme="mips:selection_type#" term="Appraisal Submission"/>
  <category scheme="mips:mdc" term="1"/>
  <leap2:spatial>Glasgow East Health Centre</leap2:spatial>
  <leap2:status leap2:stage="Planned" leap2:label="Gathering pre-meeting supporting
information" />

  <link rel="leap2:supports" href="https://www.northscotlandtrust.nhs.uk/gmc/1112222"/>

  <link rel="leap2:attended_by" href="https://www.northscotlandtrust.nhs.uk/gmc/1112222"/>
  <link rel="leap2:attended_by" href="https://www.northscotlandtrust.nhs.uk/gmc/2223333"/>

  <link rel="leap2:has_part" href="portfolio:appraisal/3242/indemntity" />
  <link rel="leap2:has_part" href="portfolio:appraisal/3242/criminal_charges" />
  <link rel="leap2:has_part" href="portfolio:appraisal/3242/last_year_overview" />
  <link rel="leap2:has_part" href="portfolio:appraisal/3242/next_year_improvements" />
  <link rel="leap2:has_part" href="portfolio:appraisal/3242/registered_gp" />

  <link rel="leap2:supported_by" href="portfolio:supporting_info/3211" />
</entry>
```

4.2.3.5. Supporting Information Example

This example uses the MIPS Supporting Information Type of 'SI Complaint'.

```
<entry>
  <title>Patient Feedback - Complaint</title>
  <id>portfolio:supporting_info/3211</id>
  <updated>2010-09-10T15:43:00Z</updated>
  <leap2:date leap2:point="target">2011-03-01T10:00:00Z</leap2:date>
  <rdf:type rdf:resource="leap:entry"/>
  <category scheme="mips:supporting_information_type#" term="SI - Complaint"/>
  <category scheme="mips:mdc" term="2"/>

  <link rel="leap2:supports" href="portfolio:appraisal/3242" />
  <link rel="leap2:has_part" href="portfolio:supporting_info/3211/summary_of_complaint" />
  <link rel="leap2:has_part" href="portfolio:supporting_info/3211/what_i_have_learned" />
  <link rel="leap2:has_part"
href="portfolio:supporting_info/3211/how_i_have_changed_my_practice" />
  <link rel="leap2:has_part" href="portfolio:supporting_info/3211/status" />

  <!-- Only the files that match the requested and providers policy MDC are included -->
  <link rel="leap2:has_evidence" href="porfolio:file/4567"/>
  <link rel="leap2:has_evidence" href="porfolio:file/4568"/>
</entry>
```

This example details a Supporting Information that has MDC 4, but the provider wishes to provide summary information (MDC 2) and a link to further MDC 4 information.

```
<entry>
  <title>Patient Feedback - Complaint</title>
  <id>portfolio:supporting_info/3211</id>
  <updated>2010-09-10T15:43:00Z</updated>
  <leap2:date leap2:point="target">2011-03-01T10:00:00Z</leap2:date>
  <rdf:type rdf:resource="leap:entry"/>
  <category scheme="mips:supporting_information_type#" term="SI - Complaint"/>
  <category scheme="mips:mdc" term="2"/>

  <link rel="leap2:supports" href="portfolio:appraisal/3242" />
  <link rel="leap2:has_part" href="portfolio:supporting_info/3211/summary_of_complaint" />
  <link rel="leap2:has_part" href="portfolio:supporting_info/3211/what_i_have_learned" />
  <link rel="leap2:has_part"
href="portfolio:supporting_info/3211/how_i_have_changed_my_practice" />
  <link rel="leap2:has_part" href="portfolio:supporting_info/3211/status" />

  <!-- Only the files that match the requested and providers policy MDC are included -->
  <link rel="leap2:has_evidence" href="porfolio:file/4567"/>
  <link rel="leap2:has_evidence" href="porfolio:file/4568"/>

  <!--Further information available (e.g. higher MDC) can be represented as a link to an
organisation-->
  <link rel="leap2:has_evidence" href="http://www.northscotlandtrust.nhs.uk" />
</entry>
```

4.2.3.6. Extension Attribute Example

All extension attributes are represented as basic 'entry' elements. The summary field should be used to store the attributes value, with the description field may be used secondarily to store

further descriptive information. For example, the speciality name would go in the summary field and the speciality description in the description field.

This example uses the MIPS Extension Attribute of 'Summary of Complaint'

```
<entry>
  <title>Summary of Complaint</title>
  <id>portfolio:supporting_info/3211/summary_of_complaint</id>
  <updated>2010-09-10T15:43:00Z</updated>
  <content type="text">
    summary information regarding the complaint, adhering to appropriate
    MIPS Data Classification (MDC)
  </content>
  <rdf:type rdf:resource="leap:entry"/>
  <category scheme="mips:mdc" term="4"/>

  <link rel="leap2:is_part_of" href="portfolio:supporting_info/3211" />
</entry>
```

4.2.3.7. Resource Examples

This is an example of a paper feedback letter that is contained within an organisation.

```
<entry>
  <title>Patient Feedback File</title>
  <id>portfolio:file/4567</id>
  <updated>2010-09-10T15:43:00Z</updated>
  <content type="text">
    Original hand written letter submitted by the patient
  </content>
  <rdf:type rdf:resource="leap2:resource"/>
  <category scheme="categories:resource_type#" term="Physical"/>
  <category scheme="mips:mdc" term="2"/>

  <spatial>North Glasgow Health Centre</spatial>
</entry>
```

This is an example of an electronic feedback letter that is available online.

```
<entry>
  <title>Patient Feedback File</title>
  <id>portfolio:file/4568</id>
  <updated>2010-09-11T15:43:00Z</updated>
  <content type="text">
    Anonymised PDF version created from patient letter
  </content>
  <rdf:type rdf:resource="leap2:resource"/>
  <category scheme="categories:resource_type#" term="Web" />
  <category scheme="mips:mdc" term="3"/>

  <link rel="enclosure" href="http://portfoliowebsite.com/file1.pdf" length="59693"
  type="application/pdf"/>
</entry>
```

5. N3 Gateway

This section defines an implementation of the MIPS standards and policies to provide a system to securely make N3 based portfolio data available for doctors' professional portfolios.

5.1. Background

Most doctors are working in an environment where the data that they are recording, referring to, manipulating and making decisions on, belongs to their employer. This data may contain a number of sensitive pieces of information most notably patient related but potentially also commercial in nature.

With appraisal and revalidation, a doctor has an individual requirement to demonstrate aspects of their working practice, in doing so they will require access to this local information as supporting evidence, alongside additional information which may belong specifically to the doctor (e.g. CPD activities).

When the doctor is required, for the purposes of revalidation, to upload supporting, potentially patient sensitive information to a system out with the NHS (e.g. to a college e-portfolio or e-logbook), and therefore not managed by the local data controller, this presents the doctor with a number of challenges and responsibilities:

- 1) They may be breaching the Data Protection Act (DPA) regulations as the doctor does not implicitly have the permission of the data controller (the trust) to transfer this data out of the organisation.
- 2) Unless the doctor is sure that the third party system is NHS compliant then they are potentially breaching National NHS guidelines. i.e. they would have to be sure that the third party system adhered to NHS guidelines (IG statement of Compliance & ISO 27001), etc.
- 3) In the absence of either of circumstances being met then potentially it leaves the doctor open to disciplinary action.

Potentially, therefore, for a doctor to proceed with certainty that they are not breaching their terms of employment or NHS guidelines they would need to establish that the system to which they intend to upload information, was NHS compliant and then confirm approval of their trust for every piece of information to be uploaded. Clearly this will be impractical and potentially

leaves the practicing doctor in an untenable position.

5.2. Description of the N3 gateway

The N3 gateway for revalidation project sets out to demonstrate a “proof of concept”.

It is designed around the consideration that the majority of the information which a doctor needs to supply as supporting evidence for revalidation, will require collection and storage, but will only be accessed in a detailed fashion on occasion, and that important summary (and non sensitive) information can be drawn from the supporting information and made available without compromising either local or national data governance rules.

Exemplar:-

Thus the typical process of handling such data through the gateway would be, for example, collection of supporting information related to a complaint; this might include; a letter from Patient, a response from the Trust, an account of the event by doctor, response to the patient by the trust, summary of outcome, etc.

In order for effective appraiser assessment of the event, it is necessary for this information to be available securely for reference, however at this stage there is no particular reason for this detailed information to leave the organisation. It is necessary though to record some information about the complaint episode; i.e. when did it happen, how long did it take to come to resolution, what was the outcome, etc. This information is important to be readily available for the doctor’s portfolio and arguably does not compromise any sensitive information (except perhaps about the individual doctor). If, subsequently, access is required to the full information it is important that the information is aggregated and accessible via an N3 compliant mechanism without the subsequent need for further manipulation of the data. It is crucial therefore that the information is pre-prepared for ready access but also transition from the N3 environment to external scrutiny, if required by the appraisal process. The unpredictable timing of when patient sensitive information will be required to leave the confines of the N3 environment for external evaluation, or any other reason, makes the conditions for storage of this data such that they are compliant with the standards dictated by statute at outset.

Therefore the model of the gateway is as follows:

- To provide a locally controlled repository of supporting information that the doctor can upload all information that they feel is relevant to gain a full understanding of the event.

This is securely retained within the repository and access to this is controlled by the local authority.

- To be able to answer some standard questions about the event, the answers to which are then available to be drawn down by one or more externally based portfolios to become part of the doctor's portfolio record. The questions asked will be defined by the standards and interoperability group thus will be consistent across the whole of medicine.
- To provide information to external portfolios on how the detailed supporting information can be accessed in the situation where further information is to be sought. This information is likely to be in the form of a unique identification number identifying the event, together with information about where the full event information is held i.e. Trust, Local Authority or National System. Access to the full (potentially containing patient sensitive information) event information then remains governed by the local authority via local mechanisms.

The Gateway will be NHS compliant and we envisage that in many cases may be run by the local authority as part (or a module) of a larger appraisal system. The contract describing what information is allowed to leave the organisation is defined by the revalidation standards definition (i.e. what questions are asked of each event) and this will be signed off by the data controller as being acceptable.

The result from the doctor's point of view is that when handling local employer owned information, they can be confident that they are not breaching either local DPA rules or national security guidelines, and that all relevant information will be transparently available to their professional portfolio held by which ever College or Organisation they wish.

5.3. Delivery, maintenance and future upgrading

This project aims to deliver an initial fully working prototype which is N3 Compliant and will run a basic set of services based on the standards work underway in order to "prove the concept". In the longer term it is envisaged that if successfully this version of the system would be maintained by the Royal College of Surgeons of Edinburgh on behalf of the surgical, Physician and General Practice communities if appropriate agreements are put in place. However the model also lends itself to be replicated and potentially incorporated into local appraisal systems run by trusts or local authorities and in this instance a commercial organisation may develop,

supply and maintain such a system.

5.4. Deliverables

As already indicated, the primary goal of the pilot is to implement a solution that communicates valuable data between 2 systems with adherence to the specification. In addition we intend to produce a number of open source libraries which will be made available to other implementations. This demonstration system will initially at least work on a peer to peer basis with direct communications between consumers and providers.

We have defined three systems/modules to be implemented as part of the initial pilot to demonstrate an N3 gateway.

5.4.1. Gateway Administration & Policy Manager

The Administration and policy manager application provides the top level administrative functions of the gateway. It is therefore not involved in any consumer or provider role, but it is required to communicate with the MIPS website from time to time to check for new standards versions and updates to the policy items.

The main function of the policy manager is to provide local management of the gateway, selecting and updating policies and standards versions from the MIPS site and allowing overriding of the policy elements in order to adhere with local policy requirements where appropriate. The main functions are therefore:

- Maintain local copies of the standard category and type vocabularies.
- Check for version updates of the standards
- Maintain local copies of the policies, including a cache of the provider list copied from the MIPS site.
- Filter the provider list if necessary to publish a subset of providers to local users.
- Check for version updates of the policies
- Manage the current “in use” versions that determine the user interface, MDC coding and mapping to data structures.
- Provide tools to override and extend policy rules for local needs.
- Manage gateway users and roles.
- Manage push notifications to consumers.
- Manage “blacklists” and potentially “whitelists” of provider and consumer systems.

Local management tools of the policy items are important to allow a local organisation to set MDC categories on data items to meet the needs of the local organisation that the gateway is serving. Although we expect that the centrally published MIPS policies will suffice in most instances there may be times when an organisation wishes to set their own different levels for certain data items or to create their own specific supporting information templates. In the future it may also be possible to have additional sets of policies for different requesting organisations, i.e. a partner organisation or another unit in a trust, thus providing fuller interoperability with trusted consumers.

5.4.2. N3 Gateway Provider System

The N3 gateway provider system is aimed at demonstrating the use of the MIPS standards in a provider role. The system is a web based system that is intended to be installed and administered in a local secure environment such as an NHS trust or other authority.

The main functions of this system are:

- Provide a rudimentary “full detail” secure repository of medical portfolio supporting information, managed by the local governing authority.
- Provide a user interface with supporting information upload forms based on the policy templates (or overridden locally created versions where applicable)
- Implement a MIPS provider layer to safely expose parts of this repository for secure copy and transfer to external medical portfolio systems.

The System will therefore include

1. Local and federated authentication mechanisms with role based access control.
2. A person repository for each registered local user with an interface to allow each user to input information according to MIPS Policy templates.
 - a. This data will be coded automatically under MIPS categories
 - b. Users will be provided guidance as to how the data will be coded and thus when they should or should not avoid entering patient or co-worker identifiable information.
 - c. Each person repository will also have a simple administration area where they will be able to view accesses to their data and revoke or block completely access to their repository from external systems.
3. A secure mechanism by which an administrator can provide a local user acting as Appraiser of Revalidation Office full access to a local users repository with the local

- users permission. This will not be via the MIPS interface but directly with the system.
4. In developing the provider MIPS components, a code library (.NET) that outputs Leap2A compliant XML will be developed and made generally available.
 5. An Implementation of the RESTful web services according to the MIPS specification.
 6. An Implementation of the OAuth API as well as providing an Access Token Generator and User Authorisation screen.

The screenshot shows the N3 Gateway web interface. At the top right, it says "Hello Paul Smith, Logout". The main heading is "Record a Complaint". On the left is a navigation menu with "Create Appraisal", "Navigation", and "Edit Profile". The form has three main sections: "Title" with a text input field and an info icon; "Valid Date" with a text input field, an info icon, and a callout box; and "Summary of complaint" with a large text area and an info icon. The callout box for "Valid Date" contains the text "Valid Date MDC: 2 This information should be...".

Figure 6: Example Provider System

The example screen above depicts a simple input screen that has been created based on MIPS Policy, the fields and MIPS Data Classification could change as policy changed.

5.4.3. MIPS Consumer demonstration implementation

The MIPS consumer system will demonstrate a system in the role of a consumer of portfolio data being held in another portfolio and being made available by the MIPS provider interface.

This system will be developed initially as a standalone web based application that will integrate with an existing portfolio database, using the existing local user authentication and security mechanism for access control. The application will provide the local users a mechanism of

requesting information from the N3 gateway provider system and updating received portfolio data into the local portfolio system.

The demonstration system shall be built around the Royal of Surgeons (intercollegiate group) electronic portfolio – Surgeons Portfolio.

The Main Features of this system are therefore:

- A mechanism to select a provider from a list and to provide credentials for that providers system to set up the authorisation to allow data to be transferred into the local portfolio
- Manage a list of providers that have been added as providers of portfolio data for this user and allow the user to remove entries where necessary.
- Provide a history of information transferred to the user.
- Provide a simple administrative interface for the portfolio administrators with such information of quantity of data items transferred, number of providers, users, etc

The following tasks will be undertaken

- Mapping of the MIPS data model to the RCS data model
- Development of .NET libraries to provide the security, REST and MIPS Object Entities.
- Connection of MIPS .NET consumer libraries to local database libraries to allow the storage and update of local portfolio items.
- Communication with MIPS provider list to download and cache the provider list.
- Provide simple administration to allow the portfolio system administrators to determine which providers to allow users to select.
- Develop user interface to manage authorisation and the provider list.

6. Appendix A – Leap2A Example

The following example demonstrates appraisal information coming from a fictional NHS Trust's, NHS North Scotland, appraisal system called Appraisals. The feed is a result of a request for MDC 3 information regarding Dr John Smith (GMC No. 1112222) between January and December 2010.

The example shows an appraisal that took place on the 15 Sept 2010, it contains a Complaint as supporting information. Links to the original complaint letter and anonymised PDF are detailed.

Medical Interoperability Portfolio Standards (MIPS)
Specification

```
<?xml version="1.0" encoding="utf-8"?>
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
      xmlns:leap2="http://terms.leapspecs.org/"
      xmlns:categories="http://wiki.leapspecs.org/2A/categories/"
      xmlns:portfolio="https://www.northscotlandtrust.nhs.uk/appraisals"
      xmlns:mips="http://www.mips.org.uk/specification/categories">

  <title>MIPS data feed</title>

  <id>https://www.northscotlandtrust.nhs.uk/appraisals/3/https%3A%2F%2Fwww.northscotlandtrust.nhs.
  uk%2Fgmc%2F1112222%20%2010-01-01%2010-12-31</id>
  <updated>2010-10-08T20:25:05-08:00</updated>

  <!-- The href point to the leap2:organisation element -->
  <link rel="mips:creator" href="http://www.northscotlandtrust.nhs.uk"/>
  <link rel="mips:data_governor" href="http://www.northscotlandtrust.nhs.uk"/>

  <!-- Primary leap2:organisation element -->
  <entry>
    <title>NHS North Scotland</title>
    <id>http://www.northscotlandtrust.nhs.uk</id>
    <updated>2010-01-12T11:03:55Z</updated>
    <leap2:orgdata leap2:field="workphone">
      0123 456 7890
    </leap2:orgdata>
    <rdf:type rdf:resource="leap2:organization"/>
    <spatial>123 Main St, Inverness, Scotland</spatial>
  </entry>

  <!-- Primary leap2:person element defined by the Self term -->
  <entry>
    <title>Smith, John, Dr</title>
    <id>https://www.northscotlandtrust.nhs.uk/gmc/1112222</id>
    <updated>2010-01-12T11:03:55Z</updated>
    <leap2:persondata leap2:field="id" leap2:service="www.gmc-uk.org/list/">
      1112222
    </leap2:persondata>
    <rdf:type rdf:resource="leap2:person"/>
    <category scheme="categories:person_type#" term="Self"/>
    <link rel="leap2:supported_by" href="portfolio:appraisal/3242"/>
    <!--
      Optional declaration of the creator and data governing organisation
      N.B. This are redundant in this example as they only repeat the feed links
    -->
    <link rel="mips:creator" href="http://www.northscotlandtrust.nhs.uk"/>
    <link rel="mips:data_governor" href="http://www.northscotlandtrust.nhs.uk"/>
  </entry>

  <!-- Addition leap2:person element -->
  <entry>
    <title>Jones, Mary, Dr</title>
    <id>https://www.northscotlandtrust.nhs.uk/gmc/2223333</id>
    <updated>2010-09-13T11:03:55Z</updated>
    <leap2:persondata leap2:field="id" leap2:service="www.gmc-uk.org/list/">
      2223333
    </leap2:persondata>
    <rdf:type rdf:resource="leap2:person"/>
    <category scheme="categories:person_type#" term="Mentor"/>
    <link rel="related" href="portfolio:appraisal/3242"/>
  </entry>

  <!-- Context Selection (Appraisal) element -->
  <entry>
    <title>Appraisal Interview</title>
    <id>portfolio:appraisal/3242</id>
    <updated>2010-09-15T11:03:55Z</updated>
    <rdf:type rdf:resource="leap2:selection"/>
    <leap2:date leap2:point="target">2011-03-01T10:00:00Z</leap2:date>
```

```
<category scheme="mips:selection_type#" term="Appraisal Submission"/>
<leap2:spatial>Glasgow East Health Centre</leap2:spatial>
<leap2:status leap2:stage="Planned" leap2:label="Gathering pre-meeting supporting
information" />

<link rel="leap2:supports" href="https://www.northscotlandtrust.nhs.uk/gmc/1112222"/>

<link rel="leap2:attended_by" href="https://www.northscotlandtrust.nhs.uk/gmc/1112222"/>
<link rel="leap2:attended_by" href="https://www.northscotlandtrust.nhs.uk/gmc/2223333"/>

<link rel="leap2:has_part" href="portfolio:appraisal/3242/indemnity" />
<link rel="leap2:has_part" href="portfolio:appraisal/3242/criminal_charges" />
<link rel="leap2:has_part" href="portfolio:appraisal/3242/last_year_overview" />
<link rel="leap2:has_part" href="portfolio:appraisal/3242/next_year_improvements" />
<link rel="leap2:has_part" href="portfolio:appraisal/3242/registered_gp" />

<link rel="leap2:supported_by" href="portfolio:supporting_info/3211" />
</entry>

<entry>
<title>Medical Indemnity Insurance Validated</title>
<id>portfolio:appraisal/3242/indemnity</id>
<updated>2010-09-15T11:03:55Z</updated>
<rdf:type rdf:resource="leap2:entry"/>
<content type="text">true</content>
<link rel="leap2:is_part_of" href="portfolio:appraisal/3242" />
</entry>

<entry>
<title>Criminal Charges Exist</title>
<id>portfolio:appraisal/3242/criminal_charges</id>
<updated>2010-09-15T11:03:55Z</updated>
<rdf:type rdf:resource="leap2:entry"/>
<content type="text">>false</content>
<link rel="leap2:is_part_of" href="portfolio:appraisal/3242" />
</entry>

<entry>
<title>CPD Overview Last Year</title>
<id>portfolio:appraisal/3242/last_year_overview</id>
<updated>2010-09-15T11:03:55Z</updated>
<rdf:type rdf:resource="leap2:entry"/>
<content type="text">Here is a summary of last years CPD</content>
<link rel="leap2:is_part_of" href="portfolio:appraisal/3242" />
</entry>

<entry>
<title>CPD Improvments Next Year</title>
<id>portfolio:appraisal/3242/next_year_improvements</id>
<updated>2010-09-15T11:03:55Z</updated>
<rdf:type rdf:resource="leap2:entry"/>
<content type="text">Here is a summary of the improvements identified for the coming
year</content>
<link rel="leap2:is_part_of" href="portfolio:appraisal/3242" />
</entry>

<entry>
<title>Registered with a GP</title>
<id>portfolio:appraisal/3242/registered_gp</id>
<updated>2010-09-15T11:03:55Z</updated>
<rdf:type rdf:resource="leap2:entry"/>
<content type="text">>true</content>
<link rel="leap2:is_part_of" href="portfolio:appraisal/3242" />
</entry>

<!-- Supporting Information (Complaint) element -->
<entry>
<title>Patient Feedback - Complaint</title>
```

Medical Interoperability Portfolio Standards (MIPS)
Specification

```
<id>portfolio:supporting_info/3211</id>
<updated>2010-09-10T15:43:00Z</updated>
<leap2:date leap2:point="target">2011-03-01T10:00:00Z</leap2:date>
<rdf:type rdf:resource="leap:entry"/>
<category scheme="mips:supporting_information_type#" term="SI - Complaint"/>

<link rel="leap2:supports" href="portfolio:appraisal/3242" />

<link rel="leap2:has_part" href="portfolio:supporting_info/3211/summary_of_complaint" />
<link rel="leap2:has_part" href="portfolio:supporting_info/3211/what_i_have_learned" />
<link rel="leap2:has_part"
href="portfolio:supporting_info/3211/how_i_have_changed_my_practice" />
<link rel="leap2:has_part" href="portfolio:supporting_info/3211/status" />

<!-- Only the files that match the requested and providers policy MDC are included -->
<link rel="leap2:has_evidence" href="porfolio:file/4567"/>
<link rel="leap2:has_evidence" href="porfolio:file/4568"/>
</entry>

<entry>
<title>Summary of Complaint</title>
<id>portfolio:supporting_info/3211/summary_of_complaint</id>
<updated>2010-09-10T15:43:00Z</updated>
<content type="text">
summary information regarding the complaint, adhering to appropriate
MIPS Data Clasification (MDC)
</content>
<rdf:type rdf:resource="leap:entry"/>
<link rel="leap2:is_part_of" href="portfolio:supporting_info/3211" />
</entry>

<entry>
<title>Learning & Development</title>
<id>portfolio:supporting_info/3211/what_i_have_learned</id>
<updated>2010-09-10T15:43:00Z</updated>
<content type="text">
Descriptive content on what&quot;s been learned
</content>
<rdf:type rdf:resource="leap:entry"/>
<link rel="leap2:is_part_of" href="portfolio:supporting_info/3211" />
</entry>

<entry>
<title>Successes</title>
<id>portfolio:supporting_info/3211/how_i_have_changed_my_practice</id>
<updated>2010-09-10T15:43:00Z</updated>
<content type="text">
Information on how the practice has changed
</content>
<rdf:type rdf:resource="leap:entry"/>
<link rel="leap2:is_part_of" href="portfolio:supporting_info/3211" />
</entry>

<entry>
<title>Improvement Suggestions</title>
<id>portfolio:supporting_info/3211/status</id>
<updated>2010-09-10T15:43:00Z</updated>
<content type="text">
Status of the complaint
</content>
<rdf:type rdf:resource="leap:entry"/>
<link rel="leap2:is_part_of" href="portfolio:supporting_info/3211" />
</entry>

<entry>
<title>Patient Feedback File</title>
<id>portfolio:file/4567</id>
<updated>2010-09-10T15:43:00Z</updated>
<content type="text">
```

```
    Original hand written letter submitted by the patient
  </content>
  <rdf:type rdf:resource="leap2:resource"/>
  <category scheme="categories:resource_type#" term="Physical"/>
  <spatial>North Glasgow Health Centre</spatial>
</entry>

<entry>
  <title>Patient Feedback File</title>
  <id>portfolio:file/4568</id>
  <updated>2010-09-11T15:43:00Z</updated>
  <content type="text">
    Anonymised PDF version created from patient letter
  </content>
  <rdf:type rdf:resource="leap2:resource"/>
  <category scheme="categories:resource_type#" term="Web" />
  <link rel="enclosure" href="http://portfoliowebsite.com/file1.pdf" length="59693"
type="application/pdf"/>
</entry>
</feed>
```