NHS
England

Open API Architecture Policy

THE NHS CONSTITUTION
the NHS belongs to us all

Open API Architecture Policy

First published: May 2014

Updated:

Prepared by NHS England Strategic Systems & Technology

NHS England INFORMATION READER BOX

Directorate		
Medical	Operations	**Patients and Information**
Nursing	Policy	Commissioning Development
Finance	Human Resources	

Publications Gateway Reference:	**01561**
Document Purpose	Guidance
Document Name	Open API Architecture Policy
Author	NHS England/P&I/Strategic Systems and Technology
Publication Date	May 2014
Target Audience	CCG Accountable Officers, Foundation Trust CEs , Medical Directors, Directors of Nursing, Local Authority CEs, Directors of Adult SSs, NHS England Regional Directors, NHS England Area Directors, NHS Trust Board Chairs, Directors of Finance
Additional Circulation List	CCG Clinical Leads, CCG Accountable Officers, CSU Managing Directors
Description	This architecture policy sets out the NHS England view on the use of "Open API" to support the delivery of software interoperability for health and care systems.
Cross Reference	N/a
Superseded Docs (if applicable)	N/a
Action Required	N/a
Timing / Deadlines (if applicable)	**N/a**
Contact Details for further information	Inderjit Singh Head of Enterprise Architecture Room 7E14 Quarry House Leeds LS1 7UE inderjitsingh@nhs.net

Document Status

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the intranet

Contents

1 Introduction 5

2 Policy Context 6

2.1 Purpose of this policy: 6

2.2 Audience for the Policy 6

2.3 Definitions and Scope 6

2.4 Governance 8

3 Policy Statement 10

4 Guidance 11

4.2 Characteristics of the API 13

4.3 Further explanation of the characteristics 14

5 Terms of Agreement and Commercial Provisions 18

Appendix: Output Based Specification (OBS) Example 25

1 Introduction

To achieve our vision of a people powered health and social care system enabled by the Integrated Digital Care Record we need an interoperable ecosystem of applications, data and processes to allow the right information to be available to the right user at the right time. The fundamental elements of the vision are:

- Transparency; safe and reliable sharing of information between clinicians, patients and the public,
- Participation; supporting patients and citizens to take more control of their health and care and fully engage in the design of local services, and
- Interoperability; to develop the capability to realise integrated digital records across all care settings.

Principles for Open Standards across government for software interoperability, data and document formats have been directed by the Government Digital Service[1]. This architecture policy sets out the NHS England view on the use of "Open API" to support the delivery of software interoperability for health and care systems in line with this wider government policy.

The importance of using an Open API approach and hence the value of the policy is to:

- Promote and accelerate innovation through the availability of data from systems
- Maximise interoperability by exposing application functionality
- Reduce vendor lock-in to closed systems.

The term Open API refers to all methods of software-to-software interaction including, but not limited to, web interfaces, direct program interfaces, batch/file drops over FTP etc.

The following sections of this document outline the context to the policy, the specific policy statements expected to be adhered to and then supporting guidance in usage of the policy. This guidance includes further explanation; a sample output based specification and also suggested commercial provisions.

[1] https://www.gov.uk/government/policy-teams/government-digital-service

2 Policy Context

2.1 Purpose of this policy:

The objective of this architecture policy is to

- Ensure that APIs are produced for commissioned systems across health and care under open principles that enable easy and transparent integration with other systems.
- Provide guidance to ensure value for money through fair, transparent commercial terms to inform the procurement process when developing, publishing and using Open APIs.

2.2 Audience for the Policy

National System Commissioners – Individuals engaged in those systems commissioned by NHS England. For this audience it will outline the key expectations in the use of APIs for appropriately open access to the functionality, data and data schemas of these nationally provided/procured systems.

Local System Commissioners – provide guidance to local organisations on the commercial arrangements for interfaces and advice when procuring local systems.

System Producers and Providers – sets out the characteristics of the API which the solution should provide, and the expected terms of engagement to which users of the API would agree.

API Consumers - sets out the characteristics of an API which would be expected for newly commissioned systems.

2.3 Definitions and Scope

2.3.1 What do we mean by “APIs” vs. “Open APIs”

The term Application Programming Interface, or API, in the context of this document is used broadly to refer to any mechanisms which allow a system or service to access data or functionality provided by another system or service. Consequently, this policy will encourage software interoperability.

The interfaces of internal subsystems are out of scope.

Open APIs are those APIs that have been exposed to enable other systems to interact with that system, and those APIs have been sufficiently documented that the available functionality is discoverable, fit for purpose and re-usable.

Open APIs may be either integrated with the host application, or an additional piece of software that exposes any proprietary APIs with an Open API equivalent (i.e. plug- in).

Open also means potential users of the API can access the API documentation free of charge and also access the API free of charge. Also that access to Open APIs or related documentation would not be subject to any Non-Disclosure Agreement (NDA).

Where access to the live API is not possible (e.g. chargeable usage applies, service level agreements are in place, or the API returns confidential data) a test environment will be provided to allow potential users to experiment and test the API.

This is not to be confused with the term “Open Source APIs” as this refers to the availability and licencing terms of the source code for any interested party to freely change, fix or modify the code[2].

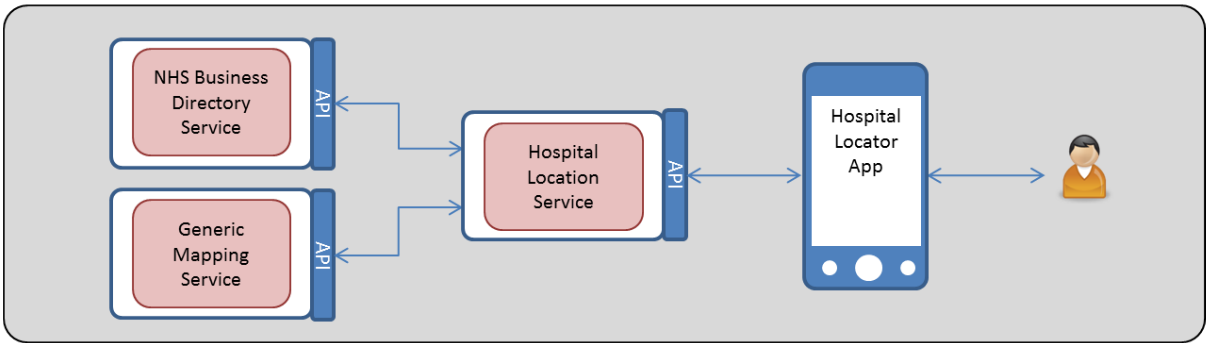
2.3.2 Licencing Models

This policy is applicable to all licencing models including Open Source, Freeware and proprietary licencing. Guidance is given to the application of the policy to the licencing model appropriate to the individual system procurements.

2.3.3 Types of Open API Usage

This policy covers both the anonymous and identified usage of Open APIs. The examples outlined below provide a further explanation of these different types of usage.

2.3.3.1 Anonymous Usage

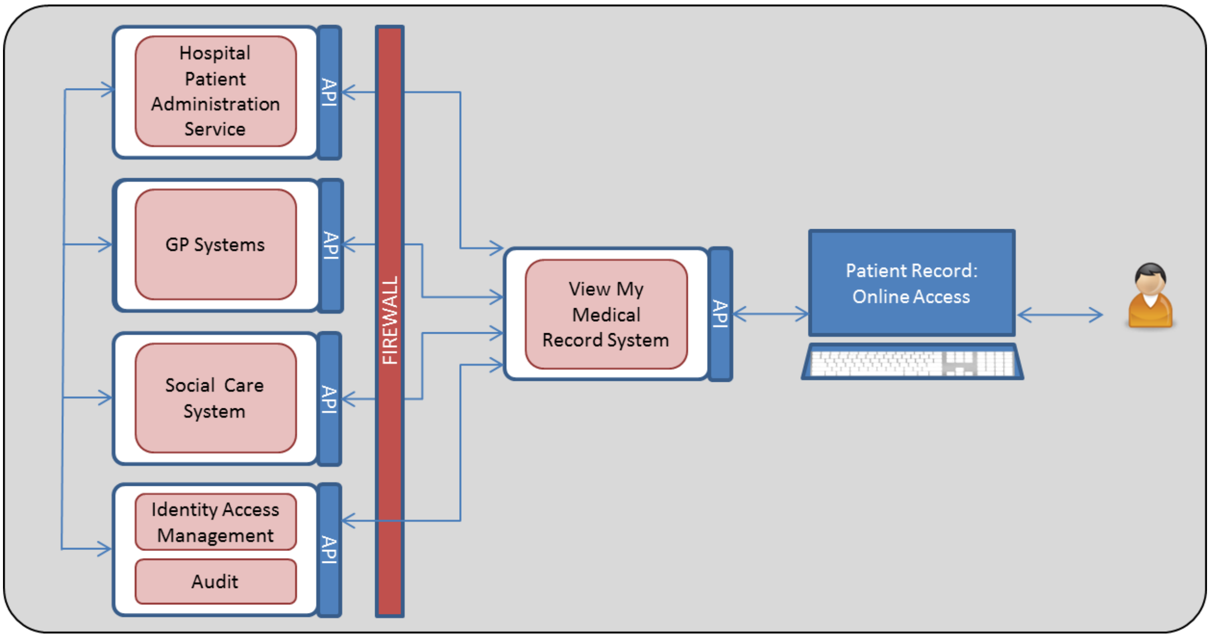


In this example a user has downloaded a Hospital Locator App onto their smart phone. This application provides the capability to search for a particular hospital with a given service and show this on the smart phone map application.

As this information is already in the public domain, the user does not need to register directly with the NHS systems. Consequently, the usage remains anonymous. The application uses the Open API that exposes the services that each hospital in the user’s area has, and combines this with the mapping data from the Generic Mapping Service to provide the Hospital Locator application the data it needs.

[2] See http://opensource.org/

2.3.3.2 Identified Usage



Hospital Patient Administration Service
API
GP Systems
API
Social Care System
API
Identity Access Management
Audit
API
FIREWALL
View My Medical Record System
API
Patient Record: Online Access

This example is more complex and shows how a system can be used to consolidate information from several clinical systems to provide an integrated view of patient data from several systems.

In this example the core hospital, GP and social care system have all exposed the patient record retrieval function through a set of Open APIs. The developer of the "View My Medical Record" system has created an application that allows the patient to view records from all three systems on a single secure portal. Due to the nature of the data being accessed, there would need to be identified access by this consuming system i.e. identified usage of the API.

2.3.4 Existing Systems

Existing system APIs may or may not meet the characteristics set out in this policy. This policy should be applied to new systems commissioned after the publication of this policy.

It can also be used as guidance to enable negotiations with the suppliers of existing systems to develop APIs to meet requirements which are considered lacking in the current implementation, therefore allowing decisions on a case by case basis to inform further system development.

2.4 Governance

For NHS England commissioned systems this policy will be part of the enterprise architecture suite of policies and principles for use in commercial and architectural governance processes.

For other commissioning bodies such as local health and care organisations this policy is provided as guidance to be applied to their relevant local governance process e.g. in demonstrating alignment to nationally funded initiatives as well as being used in establishing local best practise in support of greater interoperability.

3 Policy Statement

The policy context provided an overview of what is meant by Open APIs and the scope of the policy, This section outlines the specific policy statements and marks out a set of clear expectations for those providing and consuming Open APIs,

Ref	Policy Statement	Guidance Notes
P.1	All significant business functionality provided by the host system should be available via an Open API.	C.1
P.2	Data held by the Data Processor on the host system on behalf of the Data Controller must be made available as instructed by the Data Controller.	C.1
P.3	The existence of each exposed API must be published on publicly available resources.	C.3
P.4	Each exposed API must have freely accessible documentation that has sufficient information that would enable a competent developer has to make use of the API without further information.	C.3
P.5	Each exposed API should be accessible free of charge to enable testing. Where access to the API is chargeable and/or access is identified, developers must have non chargeable access to test APIs.	C.4
P.6	Access to confidential data, including patient or clinical data, through any API must meet, as a minimum, the same requirements for information governance, authentication and authorisation, and auditing as the host system the API exposes.	C.9
P.7	All commercial agreements relating to the development and use of Open APIs must be fair and transparent.	Section 5
P.8	Licences for usage of Open APIs by a consuming system with anonymous access must be royalty free, perpetual, non-exclusive and transferable.	Section 5
P.9	Licences for Open APIs accessing patient or clinical data by a consuming system should be non-exclusive.	Section 5

4 Guidance

This section provides guidance in the application of this policy. These guidelines outline a set of minimum requirements that should be incorporated into commercial provisions and into local operating procedures.

The different characteristics involve different actors and so it is important to understand the different roles involved in the delivery and usage of an API.

4.1 Actors

An actor is a key party, either a person or a system, which is relevant within the scope of this document.

Commissioner: The organisation procuring the system, application or software.

Producer: Responsible for delivery of the Open API related to a system. This is typically the developer of the software.

Provider: Responsible for the ongoing delivery of an operational Open API.

Consumer: Any entity that uses an Open API provided by a Producer. The consumer may be a system that itself exposes functionality and data through their own Open API. Users will be either anonymous, or identified.

Recipient: Any person that data returned from the API is disclosed to.

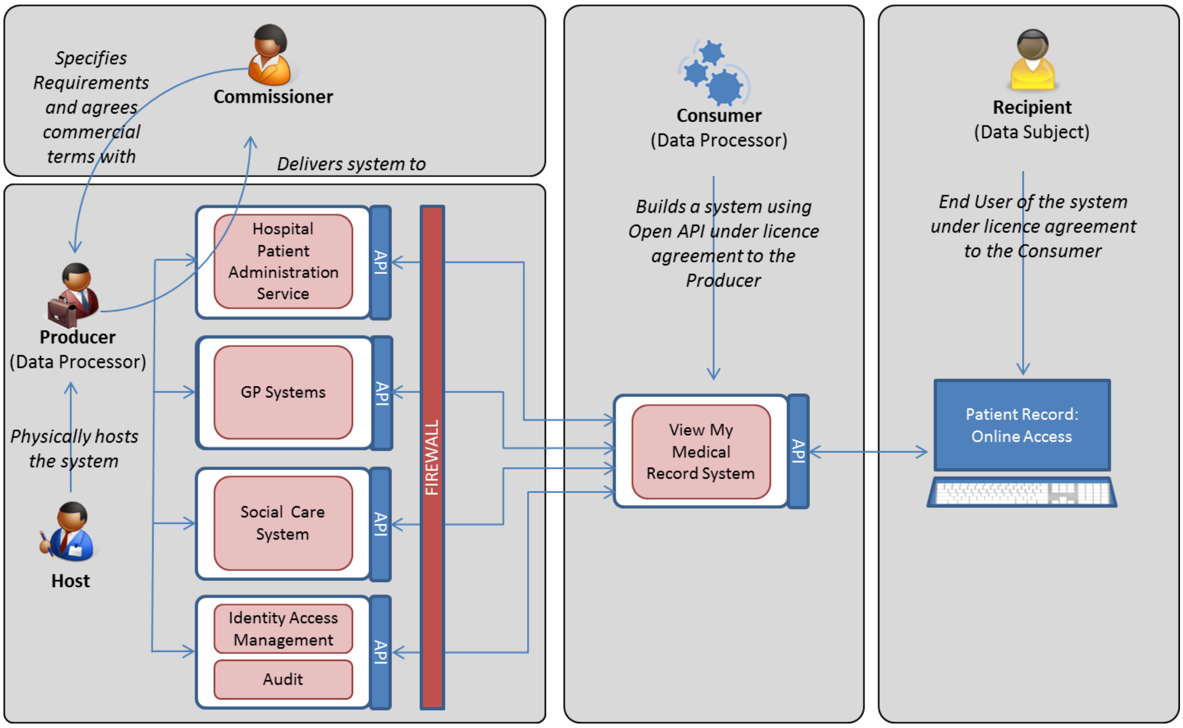
Host: The party responsible for the physical hosting of the application or system providing the Open API.

Data subject: An individual who is the subject of personal data. (DPA definition) [3]

Data controller: A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed. (DPA definition) [3]

Data processor: In relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller. (DPA definition)[3]

[3] http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions


Specifies Requirements and agrees commercial terms with
Commissioner
Delivers system to
Producer
(Data Processor)
Physically hosts the system
Host
Hospital Patient Administration Service
GP Systems
Social Care System
Identity Access Management
Audit
API
FIREWALL
Consumer
(Data Processor)
Builds a system using Open API under licence agreement to the Producer
View My Medical Record System
Recipient
(Data Subject)
End User of the system under licence agreement to the Consumer
Patient Record: Online Access

This example shows the actors and how they would interact with the "View My Medical Record" system example used in section 2.2.2. The Commissioner specifies requirements of the required core systems and also negotiates commercial terms with the Producers of each system.

The Producer has responsibilities in delivering the specified system, including the APIs, together with licencing agreements that allow open usage of these APIs. The Host physically hosts the system and may have contractual agreements with other actors to deliver against a service level agreement for those APIs. The Provider is responsible for ongoing delivery of the service.

When the Producer has delivered a system into live and exposed the APIs and relevant documentation, developers of the Consumer systems can begin to access the API documentation and access the system functionality through the APIs exposed by the Host. As previously, the developer of the Consumer system in this example has designed and deployed a system that integrates data from three systems using the Open APIs. Due to the potential differing nature of each of these APIs, each has a separate licencing agreement that the Consumer has agreed to. However, this policy will aid in providing consistency and openness of the APIs in these agreements

Finally the end user, The Recipient, registers for the service and agrees to the licencing terms for the "View My Medical Record" system. This end user licence incorporates provisions and transferable licences that the developer of the "View My Medical Record" system has already agreed to.

4.2 Characteristics of the API

This section provides an outline of the characteristics and related provisions that would be expected to be covered as a minimum within the commercial terms for delivery and usage of an API.

These can be summarised in the following table:

Reference	Characteristic	Summary	Responsible
C.1	Scope	Definition of the provided API including, usage, context and the exposed functionality.	Producer
C.2	User	If the user of the API needs to be identified or is anonymous	Producer
C.3	Documentation	Clear documentation of the API to enable developers to use the API with accompanying sample code	Producer
C.4	Testing	Testing environment(s) that developers can use.	Third party/hosting of live environment
C.5	Availability	The days and times the API will be available, and provision for planned downtime	Producer
C.6	Performance	Specify the response times for the API	Producer, Provider and Host
C.7	Usage	The number and type or requests the user should be able to make in a given time period	Host and Consumer
C.8	Quality and Accuracy	Quality criteria for the API	Producer
C.9	Access / Registration / Accreditation / Termination	The approach specifying how a user can access the API, including any requirements for accreditation	Data Controller/Data Processer/Provider
C.10	Commercial / financial considerations	Stating whether there is any charge for using the API	Producer

Reference	Characteristic	Summary	Responsible
C.11	Information Rights	Any terms and conditions regarding the use of the data acquired via the API including security, retention and destruction policies	Data Controller
C.12	Changes to the API (versioning)	How changes to the API should be managed, and permissions obtained.	Producer

4.3 Further explanation of the characteristics

C.1 Scope

All significant business functionality provided by the host system should be available via an Open API. For example, if a PAS system allows for the registration of New Patients, and Admission, Transfer and Discharge, then these functions should be available via Open APIs. The functionality exposed through APIs should be considered for each system and may be dependent on the use cases and anticipated usage of that system.

In addition functionality specific to Open APIs may be included such as the bulk extract or processing of data.

Data held in host systems by the Data Processor on behalf of the Data Controller should be made available via an Open API, consistent with the HM Government Open Data policy[4]. This should be explicitly stated in the requirements to ensure commercial terms are fair and transparent.

C.2 User

For each exposed API, there is a need to understand if the consumer of the API requires to be identified:

i) Where the user of the API needs to be identified:

Use of APIs could be restricted to use by known parties, either for information security, commercial purposes (e.g. to allow for billing for use of the API) or to provide control over the extent of usage of the API. For example, a user accessing clinical data must be identified.

ii) Where the user of the API is anonymous:

[4] For more information see the HM Government Open Data whitepaper:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/78946/CM8353_acc.pdf

The policy sets out the terms and conditions to which any user agrees to, by virtue of making use of the API. For example, a user accessing a directory of hospital services need not be identified.

C.3 Documentation

Each API should be documented to the extent that a competent developer has sufficient information to make use of the API without further information. All actions (methods) that are available through the API should be covered, as well as the legitimate data (classes) and return codes. Sample code should be made available. The documentation should be freely available.

The documentation should also cover the background to the API – an explanation of the system to which the API provides access, the general architecture of the API, the implementation plans for the API (if it is not yet available).

Description of Error codes should be provided to ensure a high quality and unambiguous user experience in case the API call returns an unexpected result.

Free registration to access the API documentation is accepted.

C.4 Testing

A testing environment (or environments if appropriate) should be provided which allows developers of the solutions making use of the API to test their solutions without affecting production environments, or an authorised process provided to support the understanding, development and testing of the API.

- Where access to the API is chargeable and/or identified, developers should have non chargeable access to test APIs to encourage innovation in the use of the API.
- Testing environments must not hold or expose confidential data, including but not limited to, live patient data.
- Free registration to access the testing environment is accepted.

C.5 Availability

For each capability of the API (method) the API agreement should specify when the API should be available. Commercial terms need to be clear on the definition of responsibilities in any service management agreement.

C.6 Performance

For each capability of the API (method) the API agreement should specify what are the Service Level Agreements (SLAs) for the response times of the API. This will be dependent on the API software and also the hosting and other dependant infrastructure, data volumes and other interfaces with systems. Commercial terms need to be clear on the definition of responsibilities in any service management agreement.

C.7 Usage

The number and type or requests the user should be able to make in a given time period, and the quality (compliance with sending well-formed requests etc.) standards required for those requests.

C.8 Quality and accuracy

The quality criteria for the API must be specified.

The API should return the same data that would be retrieved were the same function being performed within the host system. Where the API offers functionality which is not available within the host system, such as bulk data extracts, specific details of any potential inconsistencies should be clearly documented.

C.9 Access / Registration / Accreditation / Termination:

The approach specifies how a user can access the API, including any requirements for accreditation to ensure that their (proposed) access meets required standards, both technical and governance, and when such access ends.

Access to the API should be specifically set out as either anonymous or identified. Where anonymous usage is allowed, some form of usage tracking should be in place (such as IP address of calls) to allow for monitoring of usage levels. The API agreement should specify what tracking will be carried out. Where identified usage is required the API agreement should describe the process by which accreditation to use the API is carried out and the duration of such accreditation.

C.10 Commercial / financial considerations

Stating whether there is any charge for using the API or other commercial provisions.

All API agreements should set out the charges for using the API.

Anonymous usage should be free, but Identified usage may (but need not) carry charges based on the specific requirements of the host system such as a fixed rate per month, a one-off fee or a fee per usage, or per number of records, quantity of data returned, amount of resource required to process the call.

Where an API is provided free of charge the content derived from the API must be generally accessible free of charge.

Provision regarding exit criteria from any commercial obligations should be set out, specifically provisions to avoid vendor lock in.

C.11 Information Rights

Any terms and conditions regarding the use of the data acquired via the API including security, retention and destruction policies. The rights and obligations of the API user regarding all data returned by the API should be made explicit.

C.12 Changes to the API (versioning)

API should retain backwards compatibility with earlier releases. Where delivery of the API is specified by the procuring organisation; changes to the API which break backwards compatibility require the approval of the procuring organisation (or body acting on behalf of all such procurers) as per the contract.

Changes should be documented, and made publicly available.

5 Terms of Agreement and Commercial Provisions

In supporting the policy statements and the expected characteristics of an Open API, this section outlines the commercial provisions that the Commissioner will need to include relating to the API in their agreement with the Producer of the software (and with the Host unless the system is to be hosted by the Commissioning body).

The agreement with the Producer should cover:

- The functions to be supported by the API.
- The provision of access control mechanisms to ensure the API User can only use the API in conformance with their agreement with the Data Subject and Data Controller.
- The requirement to document and publish the API (or make it available for publication).
- The provision of the facilities required in the software to enable the monitoring and enforcement of agreements between the Commissioner, the Provider and/or the Host on the use of the API.
- The provision of test harness and other test facilities in the software that may be required to make a test environment available to API Consumers.
- The requirement to maintain the API (including mechanism to respond to defects and change requests).
- Provisions to avoid vendor lock in at the end of the contract, either in the case of termination or expiry.

The agreement with the Provider and the Host should cover:

- The terms and associated service levels the Host will provide in relation to the use of the API.
- The Hosts obligation to make the API available, on terms determined by the Commissioner, to those API Users (and only such users) authorised to use the API by the Customer.
- The provision of access control mechanisms to ensure the API Consumer can only use the API in conformance with their agreement with the Data Controller.
- Any provision for the Host and Provider to provide a test environment to the API Consumer.
- The terms to be offered to an API Consumer authorised by the Commissioner to use the API. This could conveniently take the form of a specimen agreement the Host would be required to offer API Consumer. This would include:
    - Service levels offered and any associated charges to the API Consumer (or other party)
    - Obligations of the API Consumer

In addition the Commissioner will need to agree with the Producer, Provider and the Host the basis on which the Data Controller will authorise the use of the API in order that the Provider and Host can ensure they are able to support such use. This would include:

- The purpose(s) for which the API Consumer may access and/or use data via the API.
- The basis on which the API Consumer may add to or update data on the system.
- The rights the API Consumer has to initiate and manage transactions via the API.
- Mechanisms by which the API Consumer will authenticate themselves to the system.
- Obligations on the API Consumer to protect any data they may have access to via the API.

All API agreements should state the terms of acceptance of the licence to use the API, standard definitions used in the API agreement, and rights and obligations of the licensee.

The following provides example provisions that should be included in the Terms of the Agreement.

For clarity, Anonymous usage refers to non-chargeable use of the API, Identified usage may be chargeable and should contain relevant commercial terms to ensure fair use, payment and associated penalty clauses as appropriate to the programme implementation of this policy.

5.1.1 Definitions

For anonymous and identified usage:

5.1.1.1 “Commercial Purposes” means any use of (xxx) for direct or indirect financial gain.

5.1.1.2 “Intellectual Property Rights” includes but is not limited to patents, trademarks, service marks, design rights (whether registered or otherwise), applications for any of the foregoing, copyright, software, database rights, trade, company or business names and other similar rights, or other right in the nature of intellectual property or obligations whether registrable or not in any country (including but not limited to the United Kingdom) ("IPR").

5.1.2 Standard Licence Terms

For anonymous usage:
The HMSO has developed a licence[5] as a tool to enable Information Providers in the public sector share and reuse information under a common open licence that may be useful.

In addition to the Open Government Licence, the following provisions should be made:

5.1.2.1 The licence terms cannot be changed by the licensor without agreement from the licensee.

5.1.2.2 Include standard clause to cover implied acceptance through continued use of an API.

5.1.2.3 Licences for anonymous usage of Open API should be royalty free, perpetual, non-exclusive and transferable.

5.1.2.4 A subsidiary system vendor will be able to grant the right to use the API to their customers on this same basis.

5.1.2.5 A licence for anonymous usage should be assignable to a third party under the Standard Licence Terms.

For identified usage:

The following provisions should be made:

5.1.2.6 The licence terms cannot be changed by the licensor without agreement from the licensee.

5.1.2.7 Include standard clause to cover implied acceptance through continued use of an API.

5.1.2.8 Licences granted for identified usage should be non-transferrable and non-exclusive.

5.1.2.9 Commercial terms over use of the API should be stated, including any royalties.

[5] Open Government Licence:http://www.nationalarchives.gov.uk/doc/open-government-licence/version/2/

5.1.2.10 Assignment of the licence to a third party will require permission from the licensor. If the permission is in writing, state so here.

5.1.2.11 The licensee is advised it is their responsibility to ensure that any third party is aware of their obligations under the Standard Licence Terms and the Licensor's IPR and the license is liable for any failure to do so.

A sample charged licence is also available from the UK Government Licencing Framework[6] for reference.

5.1.3 Licensees Obligations

For anonymous and identified usage:

5.1.3.1 Any breach of the obligations will allow the Licensor to terminate these Standard Licence Terms with immediate effect and may give rise additional causes of action.

5.1.3.2 Usage of the API must be in accordance with these Standard Licence Terms, and not use the API for purposes that, in the reasonable opinion of (Licensor), are illegal, derogatory or otherwise objectionable or that bring the (Licensor) into disrepute.

5.1.3.3 The Licensee must not represent themselves as the (Licensor). Exceptions must be clearly stated.

5.1.3.4 The Licensee must not infringe any Intellectual Property Rights belonging to the (Licensor) or alter any Producer copyright notice, trademarks, or other notices (including the terms of this Licence).

5.1.3.5 Use of copyrighted material, including the Producer logos must not be used in a way that infringes the statutory rights of any third party or in a way that misleads any third party into believing that (Licensor) is in any way or manner complicit in that infringement.

[6] http://www.nationalarchives.gov.uk/information-management/uk-gov-licensing-framework.htm

5.1.4 Non Functional Requirement Provisions

Availability

For anonymous and identified usage:

5.1.4.1 If the Service Level Agreements are to be provided on a best endeavours basis, state any relevant terms, e.g. no liability for costs or charges incurred in the event of unavailability of the API calls.

5.1.4.2 State the availability requirements clearly using:

- Days and times the service available, e.g. available between the hours of 08:00 and 19:00 Monday to Friday.

- Any requirements for special days (e.g. bank holidays)

5.1.4.3 Details of planned outage of the API, including:

- Notice period.

- Maximum time allowed for the outage. This is usually expressed as a percentage, e.g. 99% which would allow 7.2 hours downtime per month.

5.1.4.4 If the Service Level Agreement is not to be provided on a best-endeavours basis, then the agreements need to be explicitly stated.

Performance

For anonymous and identified usage:

5.1.4.5 If the Service Level Agreements are to be provided on a best endeavours basis, state any relevant terms, e.g. no liability for costs or charges incurred in the event of unavailability or unresponsive API calls.

5.1.4.6 If performance SLAs are tiered, for example guaranteed on working days, but best endeavours on weekends, provision needs to be made here.

5.1.4.7 Response time expectations of the API, e.g. 90% of calls need to be returned within.

5.1.4.8 If the Service Level Agreement is not to be provided on a best-endeavours basis, then the agreements need to be explicitly stated.

Usage

For anonymous usage:

5.1.4.9 The user of the API must agree to fair usage levels, such as how many calls can be made, either real time (human interaction) or automated (scripted) in a particular time period.

5.1.4.10 Consequences of exceeding any limits set need to be explained, for example suspension from using the service.

5.1.4.11 Process for planned usage that exceed any stated limits should be included, for example written permission requesting details of the expected extra usage.

5.1.4.12 Responsibility of the ongoing costs of the provision of the API are the responsibility of the Provider.

For identified usage, in addition to 4.2.4.7 to 4.2.4.10 above,

5.1.4.13 If agreed SLAs have been exceeded, including either total API calls, or rate of API calls, then the SLA and any associated penalty or charge related to the that SLA will be invalid.

Quality and accuracy

For anonymous and identified usage:

5.1.4.14 Any consumer of the API should not materially alter any data returned from the API. In cases where the data is adapted this should be clearly explained in the consuming application documentation.

5.1.4.15 The Licensee can expect that data returned by the API will be the same as the data which would be returned by the host system when performing that function within that system.

5.1.4.16 Where the host system cannot guarantee the quality of data (for example consistency), the API will return an appropriate warning or error message informing the user of such.

Access / Registration / Accreditation / Termination:

For anonymous usage:

5.1.4.17 State how the usage by the licensee will be monitored by the provider, (e.g. IP Tracking) to conform to the API Terms and Conditions of use.

For identified usage:

In addition to 4.2.4.15:

5.1.4.18 State how the accreditation process will be achieved.

5.1.4.19 The Provider shall not prevent or restrict any person or organisation from using the API if that person or organisation satisfies the objective, pre-determined assurance criteria as defined and published as part of the contractual arrangements.

5.1.4.20 State the auditing requirements of access to confidential data including clinical and/or patient data.

Commercial / financial considerations

For anonymous usage:

5.1.4.21 Usage of the API by The Licensee should be provided free of charge provided the terms and conditions of this licence are followed.

5.1.4.22 If usage levels or other conditions in the Terms and Conditions are exceeded, The Licensor reserves the right to make charges equivalent to costs incurred if the Licensee fails to observe these terms and conditions, or agrees in advance to usage exceeding those set out in the terms and conditions.

For identified usage:

5.1.4.23 State how the usage of the API by The Licensee will be enforced by the commercial terms and conditions.

Information Rights

5.1.4.24 Clarify who owns title, ownership and intellectual property rights.

5.1.4.25 Reference to appropriate data polices, for example retention and security

5.1.4.26 Restrictions, if any, on the reuse of data or/and data processing that create new data sets.

5.1.4.27 Obligations of the Licensee under the Data Protection Act 1998 (“DPA”) in relation to the processing, handling and storage of personal data, particularly with regard to the seventh data protection principle, and that they are not infringing the rights of any third party under the DPA.

Appendix: Output Based Specification (OBS) Example

The following is an example section of an OBS that can be used to by Commissioners of the API in specifying the requirements for Open APIs.

Requirements in <*brackets*> need to be tailored specifically to the programme.

Open API Specification

System Requirement	Details:	Delivery Priority
General		
202.1	The characteristics of the API inherit the general specification (both functional and non-functional) of the system unless detailed below.	E
202.2	*<Detail, and cross reference against which functionality must be exposed though an API>*	E
202.3	*<Measurement of usage of APIs need to be articulated. For example itmay be a count of each API used per day or hour.* *Requirements for identified >*	E
Documentation		
202.4	Documentation for the API must be publicly available, discoverable and non-chargeable.	E
202.5	*<Specify quality criteria for documentation for the exposed APIs to ensure sufficient quality that a competent developer has information to make use of the API without further information.>*	E
202.6	Documentation for the exposed APIs must include examples with executable sample code.	E
202.7	Documentation should include all error codes and related descriptions.	E
Testing		
202.8	*<Specify a requirement for testing environment that must be made available that allows potential developers using the APIs to test their solutions without adversely impacting production environments.>*	E

System Requirement	Details:	Delivery Priority
202.9	Where use of an API is chargeable, availability to a test environment must be available free of charge to the consumer.	E
202.10	*<If the Testing environment is subject to SLA, state requirements >*	E
202.11	Compliance with data security standards must be achieved, e.g. Confidential and Restricted[7] data must not be held on the test system.	E
Service Level Agreement		
202.12	*<State any temporal availability of the APIs. This may be different across APIs and may require a separate specification item.* *Also consider bank holiday holiday/special day exceptions, for example:* *The API will be available on the following time:* *Mon: hh:mm – hh:mm* *Tuesday: hh:mm – hh:mm* *Wednesday: hh:mm – hh:mm* *Thursday: hh:mm – hh:mm* *Friday: hh:mm – hh:mm* *Saturday: hh:mm – hh:mm* *Sunday: hh:mm – hh:mm >*	
202.13	*<State the requirements for uptime of the API. E.g. The API must be available 9x.x% of the working hours specified in section xxx.xx.>*	
202.14	*<State the planned maintenance requirements, e.g.* • *planned outages for maintenance, upgrades etc must be agreed n days in advance.* • *The maximum allowance for planned outage is xx minutes per month,* • *Planned outages must be performed between the hours of hh:mm and hh:mm on the following days.* • *These may only be changed by agreement with Service Management.>*	

[7] http://www.england.nhs.uk/ourwork/tsd/ig/

System Requirement	Details:	Delivery Priority
202.15	*<State the requirements for performance of the API, including* • *How it measured* • *Performance metrics, e.g x transactions per second, response time etc>*	
Volumetrics and usage		
202.16	*<State volumetric requirements, ensure these are specific e.g.* • *the rate of calls to the API will not exceed n times per second/minute/hour.* • *The total number of calls to the API will not exceed n times in each second/minute/hour.>*	
Quality and Accuracy		
202.17	*<State requirements for quality of the data provided by the API>*	
Acknowledgments		
202.18	*<State requirements for acknowledgements, e.g. Where an API is updating information, an acknowledgement of a successful update must be sent to the requesting system on successful update.>*	
Error Handling		
202.19	*<How are errors handled>*	
Access/Registration/Accreditation/Termination		
202.20	*<State requirements related to Identity Access Management and authorisation of usage, including:* • *Patient Consent* • *Auditing* • *Accreditation details* • *Usage* *>*	
Commercial Requirements		
202.21	*<State requirements to support any commercial agreements.* *Any auditing or traceability of support measuring and/or enforcement of SLA should be detailed.>*	
Non Functional requirements		

System Requirement	Details:	Delivery Priority
202.22	*<State any specific non-functional requirements not covered in the sections above, including* • *Hosting requirements* • *Disaster Recovery* • *Business Continuity* • *Maintenance* • *Etc.* >	