

Document filename:	Technical Specification for Digital Interoperability Platform		
Project / Programme	API Management	Project	
Document Reference			
Project Manager	[REDACTED]	Status	Approved
Owner	[REDACTED]	Version	1.0
Author	[REDACTED]	Version issue date	27/11/2023

Technical Specification Digital Interoperability Platform – use of API Management Platform

Document management

Revision History

Version	Date	Summary of Changes
V0.1	08/08/2022	Initial draft by [REDACTED]
V0.2	16/12/2022	Draft following agreement to proceed and with handover of PTEL lead to [REDACTED]
V0.3	17/1/23	Final edits
V0.4	23/4/23	Responses to comments
V0.5	30/5/23	Review of responses to comments
V1.0	4/9/23	Final adjustments

Reviewers

This document must be reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version
[REDACTED]	Principal IG Specialist	13/10/2022	V0.1
[REDACTED]	Solicitor PTEL	11/1/2023	V0.2
[REDACTED]	Principal IG Specialist	13/1/2023	V0.3

Approved by

This document must be approved by the following people:

Name	Signature	Title	Date	Version
[REDACTED]		IAO	27/11/23	V1.0

Glossary of Terms

Term / Abbreviation	What it stands for
API	Application Programming Interface
DIP	Digital Interoperability Platform Direction
DPIA	Data Protection Impact Assessment
IP / Client IP	IP is the network address of a computer
PII	Personally Identifiable Information

Document Control:

The controlled copy of this document is maintained in the NHS England corporate network. Any copies of this document held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity.

Purpose of document

This document sets out the technical specification for use of the Digital Interoperability Platform (DIP) as the legal basis for operation of the API Management Platform for 3rd parties. It should be read alongside the:

Establishment of systems: Digital Interoperability Platform 2019 issued by the Secretary of State for Health and Social Care.

Introduction / Purpose of service

The API Platform is a capability that allows organisations that work with health and social care to publish data and services, allowing others organisation to access (consume) such data. The publisher, who already have a legal basis for their service, will control which companies can access the data.

Currently only NHS England can publish data through the platform and this specification is to extend that to allowing other organisations (third parties) to publish their APIs via the API Platform. There are many benefits, but the notable ones are saving those organisations time and money and making it significantly easier for other organisations to onboard and consume the APIs. API consumers find that onboarding is the biggest barrier to entry (both in time and costs).

The contract NHS England has with the API Management Platform (Apigee, Google) allows such 3rd party usage.

For more details on the service and its benefits to the health and care system, see <https://digital.nhs.uk/services/api-platform>.

The intention is to open up the NHS England API platform so that it can be used by other health and care providers (public and private bodies), so long as their APIs are for the benefit of the public sector health and care system. Examples of potential third-party publishers are NHS Business Services Authority (BSA), UKHSA (UK Health Security Agency), MHRA (Medicines and Healthcare Regulatory Agency), DHSC (Department for Health and Social Care) and NICE (National Institute for Health and Care Excellence).

This would allow the wider health and care system to take advantage of the significant investment NHS England has already made in the API platform.

The “on-boarding” process for these 3rd parties is facilitated within the API Management Platform. This will allow a single governance process, set of products (approvals, status etc..) to be held by NHS England and, for Transparency, through the API Catalogue which will refer to the 3rd parties. This is augmented by the 3rd parties' own websites which will publish information on their assets for which they are responsible.

Recipients

The recipients are intended to be other NHS providers/ Social Care organisations that have technology services that can benefit from making access simpler and quicker.

It is also anticipated that future uses cases might warrant private organisations (that have not been commissioned by NHS England) publishing National APIs on this same platform.

System Delivery Function

The NHS England API platform is a ‘front door’ for health and care APIs. APIs are used by point-of-care applications and patient-facing applications to talk to back-end applications.

The platform provides a consistent experience for API consumers and API publishers (producers) that makes integration easier and supports:

- NHS England's Open API policy
- In-built use of Care Identity Service (CIS2), and NHS login national identities
- Uplifts security because there is a National view of API usage
- Operates GP Connect, which has a direction to allow third party API publication

The API Platform not only provides a single-entry point to NHS related APIs, but part of that platform there is a “Digital Onboarding Service” that:

- Provides a single place to manage integration, for both API consumers and publishers
- Fully digitises the complex assurances required to safeguard access to APIs
- Enables multiple teams to collaborate in the onboarding process
- Allows API publishers to manage their own assurance and grant access to their data without requesting NHS England manual intervention

There is an existing “API Management Platform DPIA” that defines the many aspects of the platform. The platform is based on a Commercial Off the Shelf (COTS) cloud-based solution to reduce running costs although this makes the DPIA more complex

More details can be found here: <https://digital.nhs.uk/services/api-platform>

A Platform Agreement is in place to ensure clarity of understanding of data protection and confidentiality issues and, single governance process (joint NHS England + 3rd party onboarding process), products (approval for each 3rd party, launch of each 3rd party API and uptake by a consuming organisation) and Transparency.

Data processing

The platform acts as a gateway to backend-applications published on the platform. There is no intent to analyse or store data in transit through the gateway. However, to make technical integration easier, secure the platform, improve security of the backend services, and offer technical support the platform does store some data, some of which is personally identifiable.

Categories of data

As with any solution, there are multiple groupings of data:

1. Data in-transit through the service:
 - Patient and staff data – can be any data, including unique identifiers
 - Can include patient **special category**

2. Data processed by NHS England for **security, configuration and configuration backup**
 - Patient and staff data – limited to unique identifiers
 - Where searching is involved, it could include items such as Date of Birth, Postcode, etc.
 - Technical data such as Client IP
 - System credentials to enable secure access to the APIs
3. Data processed by the API Platform held in the cloud hosted by Google
4. Data for the Digital Onboarding Service - enabling API Consumers to self-serve as much as possible during onboarding, assurance, and configure their technical connections to NHS England.
 - API publishers will also use this to manage the approval of their API Consumers

NHS England processing

Data in-transit through the service:

Data is encrypted end to end through the service. However, at the gateway level, it must be de-crypted (in-transit) for the technical functions to be carried out.

On occasion NHS England might be requested to look at live traffic for fault diagnosis. The platform significantly limits the amount of access.

No special category data is ever stored.

Data held by NHS England for security, analysis, configuration and configuration backup:

Standard range of data held (by any software provider) to support a cloud solution – including some PII. Access to this data is heavily restricted.

Data retention is 90 days.

There is a redacted (anonymised) dataset held for longer, to enable trend analysis and drive any detailed reporting.

Data held by Google to enable the operation of the cloud product:

Data held is very similar to what NHS England hold, as part of their standard cloud service

Data retention is 90 days, but the data is only used as requested by NHS England

Data to enable third parties to onboard, be assured, and configure technical connections to NHS England:

- The minimum data required is a name and email address
- Other data (such as company name), contact details are requested only when appropriate.
- There is no patient data involved

Legal basis

Data is processed pursuant to the Establishment of systems: digital interoperability platform 2019 Direction.

The data to be processed to deliver the services includes personal data and is subject to the UK GDPR.

Where a third-party API is published through the NHS England API platform, that third party would:

- Be asked to confirm their legal basis for the service
- Be a data controller for any personal data that is processed

NHS England records data to enable it to perform certain management functions as part of the API platform, which means that under UK GDPR, it would be considered joint data controller with the API provider, rather than purely as a data processor. For example, NHS England has significant control over the use of transactional data for security countermeasures.

Consultation

The question about supporting third party API publishers has come up a number of times internally. NHS England seeks to reduce the burden on the Health Sector in system delivery. It is considered that supporting third party API Publishers in the health sector would support a coordinated approach to the delivery Health Sector APIs.

Internal to NHS England the consultation has included Legal, Cyber Security and the Privacy, Transparency and Trust sub-directorate.

External discussions have occurred with the NHS Business Services Authority (BSA), NHS Wales and NHS Scotland. They have shown interest at varying levels.

Change control process

General changes to this Specification will be managed by NHS England.

Significant changes such as new categories of publishers/recipients and purposes (e.g. non-health related and social bodies) will be managed by NHS England in conjunction with the DHSC to ensure such changes are aligned with the Directions.

For any change, an update to the Direction Specification will be published.