Technical Specification for NHS Wayfinder Services

Improving lives with data and technology

Document filename:	**NHS Wayfinder Services Technical Specification V6**		
Project / Programme	**NHS Wayfinder**	Project	**Architecture**
Document Reference			
Project Manager	**REDACTED**	Status	**FINAL**
Information Asset Owner	**REDACTED**	Version	**6.0**
Author	**REDACTED**	Version issue date	**19/06/2025**

Document management

Revision History

Version	Date	Summary of Changes
6.0	19/06/2025	Version approved

Reviewers

This document must be reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version
REDACTED	Cyber Security Lead, NHS England	02/02/2026	5.2
REDACTED	IG Lead, NHS England	16/01/2026	6.0
REDACTED	Senior Associate Solicitor, NHS England	10/12/2026	5.2
REDACTED	Information Asset Owner, NHS England	19/06/2025	6.0

Approved by

This document must be approved by the following people:

Name	Title	Date	Version
REDACTED	Programme Director, NHS England	19/06/2025	6.0
REDACTED	Deputy Director Information Governance, NHS England	03/06/2025	6.0

Glossary of Terms

Term / Abbreviation	What it stands for
AES-256	*Advanced Encryption Standard*
API	*Application Programming Interface*
AWS KMS	*Amazon Web Services Key Management Service*
DPSe	*(NHS England's) Data Processing Service (evolved)*
e-RS	*NHS e-Referral Service*
MVP	*Minimal Viable Product* live Wayfinder service, in production since Sep 2022
MYR	*Manage Your Referral* patient-facing web application for electronic referrals
NEWLICS	*National Elective Waiting List Information and Contact Service*
ODS	*Organisation Data Service*

PAS	*Patient Administration System*
PEP	*Patient Engagement Platform*
PIFU	*Patient initiated follow up*
SUS	*Secondary Uses Service*
UBRN	*Unique Booking Reference Number*

Document Control:

The controlled copy of this document is maintained in the NHS Digital 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.

Contents

Introduction

The Wayfinder Programme aims to develop and deliver a solution that enables citizens to access information about their elective care via the NHS App and its associated citizen-facing delivery channels such as the NHS App and the NHS website. The key driver is the growing elective care waiting list and the need to keep citizens informed and empowered to manage their elective care pathway.

Purpose of Document

This document sets out the Technical Specification for the (Wayfinder) Services and should be read alongside:

- NHS Wayfinder Requirements Specification
    - which describes the functional and non-functional requirements for the Product (i.e. the Wayfinder service).
- NHS Wayfinder Services Directions 2023
    - which enables NHS England to provide a service to NHS patients in England to securely view summary details of their scheduled appointments with NHS Trusts and to enable them to access further details about those appointments.

Objectives

The objectives of this Technical Specification are to:

- describe how high-level business scenarios translate into technical requirements.
- present the technical solution focusing on areas that are of key relevance to Information Governance including data, information flows, and security.

Audience

The primary audiences for this document are:

- NHS Wayfinder Programme
- NHS App and NHS Account Programme
- NHS login Programme
- NHS England

Department of Health and Social Care

Technical Requirements

This section provides an overview of how key business requirements translate into high-level technical requirements. This is demonstrated by identifying architecture implications of the high-level scenarios (business use cases) as shown in Table 1.

Table 1. Architecture implications of key high-level scenarios

High-level scenario	Architecture Implications
User wants to access any Wayfinder functionality (covers all subsequent scenarios)	• Assumes patient identity is assured and proofed via NHS login
User wants to access content surfaced in the NHS App via deep link (covers a subset of subsequent scenarios)	• Driven by deep link functionality - built on existing NHS App web integrations - to hand off to specific services to enable view, edit and cancel functions • Deep link functions as a "pointer" sent by Patient-Facing Systems that will resolve directly to the relevant resource (e.g. appointment, document or questionnaire) within the Patient-Facing System
User wants to request a follow up appointment	• Requires connectivity to an internal NHS England Data Store to consume statutory returns data of patients on a patient initiated follow up (PIFU) pathway (e.g. Trust, speciality, duration of PIFU etc.) • Requires connectivity to NEWLICS to access • Requires the ability to match waiting list minimum data set PIFU information for a user for the ability to access a request process
User wants to view their appointments or referrals	• API integration with NHS England data for referrals and appointments • API integration with patient facing system providers / NHS data sources providers for any appointments • Addition of Wayfinder screens in the NHS App, bringing together data from multiple sources for a single, easy-to-use, patient view • Integration with Organisation Data Service (ODS) for up-to-date organisation information • Past appointments received from patient facing systems / NHS data sources[1] are forwarded to NHS App • De-duplication of past appointments received from patient-facing systems and NHS England data
User wants to book, change and cancel secondary care appointments	• Driven by deep-link functionality - built on existing NHS App web integrations - to hand off to specific services to enable edit and cancel functions or provided by direct integration with NHS data sources • Existing Manage Your Referral (MYR) synchronous-booking functionality re-used • Mixture of synchronous and asynchronous rebooking and cancellation journeys presented within Patient Facing Systems

[1] An **NHS data source** is a centralized repository or system that collects, stores, and provides access to structured health and administrative data used for patient care, service planning, and performance monitoring—examples include the Personal Demographics Service (PDS), Secondary Uses Service (SUS), and Waiting List Minimum Data Set (WLMDS).

User wants to access relevant resources whilst waiting for care	• Driven by deep-link functionality - built on existing NHS App web integrations - to hand off to specific services to enable edit and cancel functions • Dynamic presentation of Trust-curated documents to patients via App, based on Specialty - available within patient-facing systems only
Provide a single point of contact for the relevant appointment or referral for patients	• Driven by deep-link functionality - built on existing NHS App web integrations - to hand off to specific services to enable edit and cancel functions • Dynamic presentation of Trust contact details, based on appointment • Single point of contact for referrals and appointments Single point of contact as driven by patient-facing systems is curated by the Trust themselves via existing content management tooling
User wants to view their clinical documents (including but not limited to: allergies and adverse reactions; medicines; test results; consultations and events; other documents and correspondence)	• Driven by deep link functionality or integration with NHS data sources • Dynamic presentation of document metadata (e.g. name, type, status) and connection to other relevant events (e.g. appointments) • Requires connectivity to document back-end systems. • In some scenarios, requires connectivity to Patient Care Aggregator to retrieve document metadata (e.g. name, type, status and deep link) and enable patient to access document content and feature set via deep link
User wants to view and complete questionnaires	• Driven by deep link functionality or integration with NHS data sources • Dynamic presentation of document metadata (e.g. name, type, status) and connection to other relevant events (e.g. appointments) • Requires connectivity to document back-end systems. • In some scenarios, requires connectivity to Patient Care Aggregator to retrieve document metadata (e.g. name, type, status and deep link) and enable patient to access questionnaire content and feature set via deep link
User wants to be notified when something surfaces in the NHS App that needs their attention (NHS Notify and NHS App Notification Service)	• Native NHS App push notifications to be used by the various integrated services in the NHS App to alert users when something needs their attention, including creating a message in the App's secure message inbox where relevant • Non-app notifications (e.g. SMS, email) used as a parallel/fall-back option to ensure users can be notified in the scenario where they do not have the NHS App installed or have NHS App push notifications switched off so that user can access native patient-facing system as needed. • This requires integration between 3rd party notification workflow (managed by Patient-Facing System on behalf of a Trust) and NHS Notify / NHS App Notification & Messaging service to deliver full notification coverage and

	fall-back between options. Should this apply, it requires the ability for NHS App to inform workflow that a user does not have App installed or has their App push notifications switched off to enable fall-back coverage (including ultimate fall-back back to Trust, e.g. phone call and/or sending of letter).
Users want a single place to access, view and respond to messages they receive through the NHS App	• Leverages NHS App Message hub, a national messaging service for people who use health and care services in England to safely and securely receive communications from their healthcare providers and other national health services. Initially available to users of the NHS App who have fully verified their identity. • Securely receive, store and present message content containing personal and clinical information from third parties. • Enable users to reply to a message, with features such as keyword replies and free text replies. • To ensure that patients receive and process information about their health and care, we need to track the delivery status of the messages received and inform the sending services in a timely manner. • To help sending services determine the best way to communicate with a patient, we need to report on if a recipient of a message is using the NHS App to receive messages. • Requires integration between Patient-Facing Systems / trust systems and NHS App to populate messages sent to users with relevant message information and point the user towards a deep link to the Patient-Facing System in which they can access content such as documents, questionnaires and appointments • Note: The message content is effectively a black box to those building and running the service and is not used for any other processing.
User wants to be able to view waiting times for their expected future appointments	• Requires connectivity to NHS Data Store to consume statutory return wait list information at varying levels of detail (e.g. Trust, speciality, etc.) • Requires connectivity to waiting time data within NHSE systems to access the latest waiting list data from Trusts. • Requires the ability to match waiting time data sets for a user to provide personalised estimated wait times (e.g. for a specific speciality/trust) to users.
Provide the ability to offer and accept a PIFU pathway to a patient	• Requires connectivity to NHS Data Store to consume statutory return data of patients and identify if they may be suitable for a PIFU pathway (e.g. Trust, speciality etc.) and invite them to join a PIFU pathway • Requires the ability to notify providers of those who agree/are suitable and their management records are updated

Provide the ability for identified patients to confirm that they still require their place on a waiting list	• Requires connectivity to NHS Data Store to consume statutory return data of patients and identify if they are on a waiting list (e.g. date added to waiting list) and asking them if they are still waiting / happy to be removed from the list • Requires the ability to notify providers of those who agree to be removed from waiting list and their management records are updated
Provide the ability for identified patients to request a transfer of their care to another provider	• Requires connectivity to NHS Data Store to consume statutory return data of patients and identify if they are suitable patients for transfer of care and asking them if they would like to be moved • Requires the ability to notify providers of those who agree to be move and their management records are updated
Provide the ability for patients to access additional functionality offered through integrating parties	• Requires connectivity with integrating sources that have patient facing functionality • Requires the ability for patients to navigate to third party functionality
Provide guidance to the users as to why their information (e.g. appointments, documents, questionnaires) may not be showing and guide how the appointment tooling works	• Presentation of guidance on the Patient Care Aggregator screen in the NHS App • Presentation of guidance for under-16 users attempting to use the NHS App
Provide a mechanism by which users may provide feedback	• Inclusion of pop-up survey in NHS App

Technical Solution

This section describes the technical solution to deliver the capabilities and features of the Wayfinder service as outlined in the Business Case.

The focus of the document is on the logical aspect of the design, showing components, integrations, data flows, and security controls.

Logical Architecture

Patient Care Aggregator

The Logical architecture comprises multiple components (systems and services) that are integrated to deliver the overall Wayfinder service. This is shown in Figure 1.

These components are as follows:

- **NHS England Systems**

- **NHS login** – an Identity and Authentication service, which provides patients with a simple, secure and reusable way to access approved digital health and care services.
- **NHS App** – a national service that provides citizens in England and the Isle of Man with access to a range of NHS services both on their mobile devices and desktop computers.

  For performance monitoring, the NHS App uses cloud performance monitoring software to manage and monitor the platform. NHS App also uses this software to send log and audit data to the Cyber Security Operations Centre (CSOC).
- **API Platform (a.k.a. API-M)** – is a 'front door' for health and care APIs, primarily for NHS in England.
- **Patient Care Aggregator** – is a back-end service, designed specifically for Wayfinder, that retrieves patient data from the NHS data sources and patient-facing systems and aggregates those data for presentation in the NHS App (i.e. the front-end service).
- **NHS Data Sources** – national or trust level systems that contain information that can be used for direct care
- **Patient facing system** - are patient-facing systems that allow patients to access and manage their health care via patient engagement portal or web application.

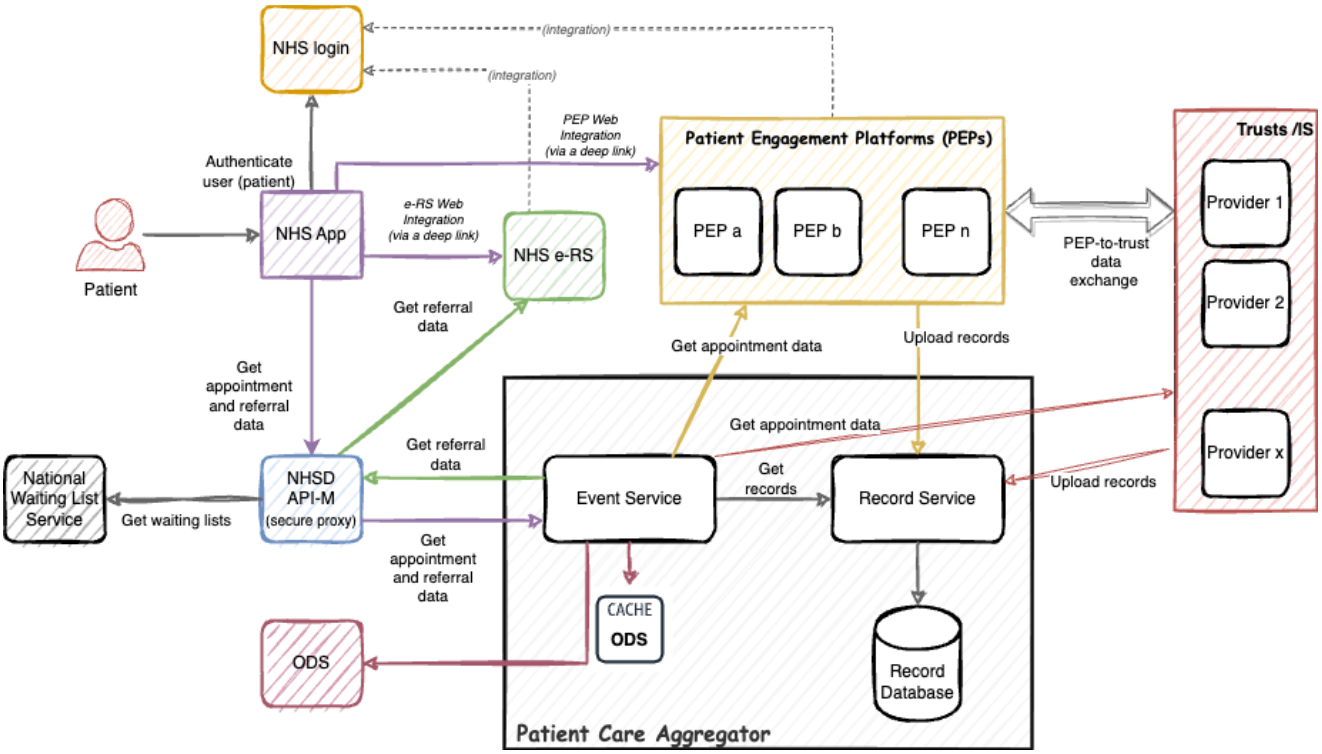

Figure 1. Wayfinder MVP Logical Architecture

The architecture has further evolved as shown in **Error! Reference source not found.** to deliver the remaining capabilities of the original Business Case. On the diagram, the new and updated integrations are shown in red.

The remaining capabilities are:

- **NHS Notify / Notifications and Messaging** – the ability to send notifications and messages to patients via the NHS App.
- **Documents and Letters** – enabling patients access to documents and letters related to their appointments.
- **Questionnaires** – providing patients with access to questionnaires related to their appointments.
- **Waiting Lists and estimated Wait Times** – providing patients with information regarding their wait list status and expected wait times if they are awaiting elective care and to allow them to confirm they still require a place on the list or to indicate a preference for transfer of care
- **PIFU** – providing patients the ability to request a follow up appointment or to request to opt into a PIFU pathway.

Table 2 provides a summary of all integrations in Wayfinder.

Table 2. Wayfinder integrations

Integration	Description
Get appointment, referral and waiting list data	Integration between NHS App and Patient Care Aggregator (via API-M). Allows retrieval of appointments and referrals together with supporting artefacts and information (such as documents, questionnaires, or waiting list data) in aggregated form.
Get referral data	Integration between Patient Care Aggregator and NHS England systems (via API-M). Enables retrieval of patient referrals.
Get appointment data	Integration between Patient Care Aggregator and patient-facing systems. Enables retrieval of patient appointment information.
Get past appointments data	Integration between Patient Care Aggregator and NHS England data (via API-M). Allow retrieval of all past secondary care appointments for the patient
Push Notifications and Messages	Either through integration of patient-facing systems with the NHS App's *Notifications and Messaging* / Notify APIs. Enables patient-facing systems to push native NHS App notifications to the user, as well as send messages to their NHS App message inbox. Also allows patient-facing systems to receive real-time status updates on the notifications and messages they send. Or, through integration with NHS data sources and NHS Notify the NHS App pushes notifications to the user, as well as send messages to their NHS App message inbox

Get document data	Integration between Patient Care Aggregator and patient-facing / Trust systems. The API published by each patient-facing system allows retrieval of documents related to the patient's appointments.
Get questionnaire data	Integration between Patient Care Aggregator and patient- facing / Trust systems. The API published by each patient-facing system allows retrieval of questionnaires related to the patient's appointments.
Upload records	Integration that enables patient- facing / Trust systems to send record locators to Patient Care Aggregator. Record locators provide information about where appointment data, documents and questionnaires can be retrieved from for a specific patient.
Get waiting list data	Presentation of indicative wait lists' statuses and wait times to the patient
Request a patient initiated follow up	Presentation of a patient's placement on a PIFU pathway and provides a mechanism to request a follow up pathway
Request to be placed on a PIFU pathway	Presentation (for identified suitable patients) of the suitability of the patient to be placed on a PIFU pathway and the ability for the patient to indicate their preference
Request for transfer of care	Presentation (for identified suitable patients) of the ability to transfer their care to another provider and the ability for the patient to indicate their preference
Request to be removed from a waiting list	Presentation (for identified suitable patients) of validation of their waiting list need and provide the ability for the patient to indicate their preference

Reporting Service

The Wayfinder Reporting Service is a bespoke architecture component, a back-end service which receives the Management Information (MI) events from the collaborating systems and services, such as patient-facing systems, Patient Care Aggregator, and the NHS App.

The Reporting Service also includes a pseudonymisation component and a data-linkage component.

The logical architecture also defines a data warehouse for storing the events, analytics tools, and a platform for the visualisation of the reports. These components are shown in Figure 2 as the Analytics and Reporting Platform.

This architecture segment is currently implemented as a local solution. The intention, however, is to transition everything to the right of the Wayfinder Reporting Service component to one of the shared analytics platforms before Q4 FY 24/25.

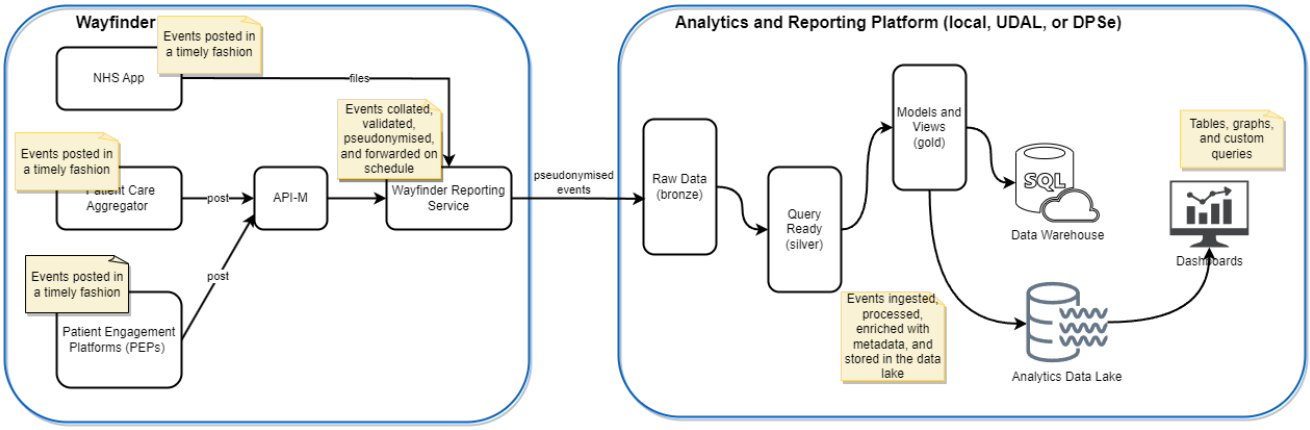

Figure 2. Logical Architecture for the Reporting Service

National Elective Waiting List Information and Contact Service (NEWLICS)

The National Elective Waiting List Information & Contact Service is a bespoke architecture component, a back-end service which stores the current national waiting list from NHS Data sources. This is utilised by other NHS services to display information to a citizen about their wait.

From these citizen facing services, a front-end questionnaire service can be accessed to enable a citizen to enter information about their care needs which are then returned to the care provider to be actioned.

The logical architecture defines a data store, a questionnaire user interface, a notification service to integrate with NHS Notify and provider integration methods. These components are shown in 4 as the National Waiting List Service.

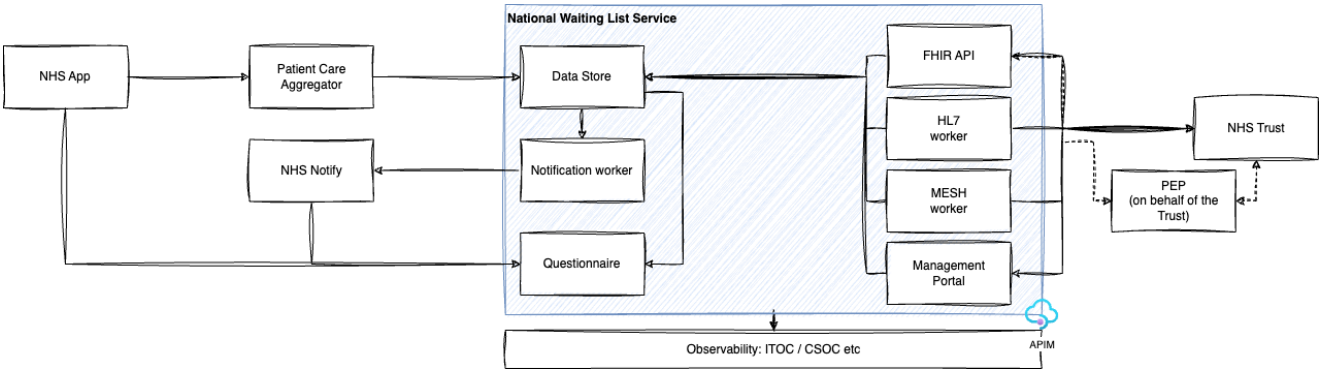

Figure 4. Logical Architecture for the National Waiting List Service

Reference Data Service

The Reference Data Service matches the ODS code to a patient readable trust name.

Data

Patient Care Aggregator

This section describes, at a high level, the data exchanged between various components of the Wayfinder service, as well as the data stored in its databases.

Outside the scope of this document are the data exchanges between NHS Trusts and their patient-facing systems.

All Patient Care Aggregator data exchanges are carried out using APIs.

Table 3 provides a more detailed description of the key data items exchanged via various APIs. The data described is indicative and should not be regarded as an exhaustive list of data items.

Acronyms used in the table are:

- Retention – indicates whether data is:
  - stored in a *database* (long periods)
  - stored in a *cache* (short periods)
  - *transient* (not stored, only transformed for display on the user's screen)
- AGG – Patient Care Aggregator
- APP – NHS App
- NECS – North of England Commissioning Support NHSE System – one of the national systems or services managed centrally by NHS England

Table 3. Key data items exchanged over APIs

Description	Source	Destination	Data items	Retention
Upload records	Patient-facing system	AGG	Patient-facing system identifier NHS Number	Database
Retrieve basic appointment detail	AGG	Patient-facing system	NHS Number NHS login's ID token Date Time Specialty Clinic Organisation Status Deep link to patient-facing system	Transient
Retrieve past appointments data	AGG	NHS E System	NHS number CDS Id Date of birth Attendance date Arrival time Expected appointment duration Outcome UBRN Care Pathway Id Consultant Code Provider Consultation medium used Site code Priority type Main specialty code	Transient

Retrieve basic referral detail	AGG	NHS E System	NHS Number NHS login's ID token Date Time UBRN Service name Organisation Consultation medium Specialty State Deep link to MYR	Transient
Discover where patients' appointment records are located	AGG	AGG	Patient-facing / Trust / NHS / independent sector system identifier NHS Number	Transient
Retrieve organisation's name	AGG	NHS E System	ODS code Organisation name	Cache
Push Notifications and Messages	Patient-facing system or NHS data source integration with NHS App	APP	NHS Number Notification text Message text	Database
Get document data	AGG	Patient-facing system	NHS Number NHS login's ID token Appointment identifier Document identifier Document date Document name Document type Document status Reference to pathway Patient-facing / Trust / NHS system identifier Deep link to a document	Transient
Get questionnaire data	AGG	Patient-facing system	NHS Number NHS login's ID token Appointment identifier Document identifier Document date Document name Document type Document status Reference to pathway Patient-facing / Trust / NHS system identifier Deep link to questionnaire	Transient

Wait Times	National Waiting List Service	AGG	NHS Number NHS login's ID token Pathway Identifier Treatment Function Code Start Date Organisation Code Site Code Census Date PIFU start date PIFU end date	Transient

Collection, processing, and storage

In summary:

- All data is collected from multiple sources via well-defined APIs published on and managed by the API Platform (API-M)
- The data sources include, but are not limited to NHS Trusts, Patient Facing Systems, NHS England Systems and NHS England Commissioned Services.
- Personal Identifiable data is stored in encrypted databases for longer periods (years) or encrypted caches for shorter periods (minutes or hours). Pseudonymised data is also stored for medium periods (months) in encrypted logs to support successful live service operations such as monitoring or incident troubleshooting. Anonymous data is stored in encrypted databases for longer periods (years) for Management Information reporting purposes.
- A feed of past appointment data will be held locally until a migration to a strategic platform can be made. This data will be held pseudonymised in an encrypted datastore.
- Data is used to enable the presentation of the required and accurate care information to the patients and exchanged across the various touchpoints between the integrated systems and components in an encrypted form
- Access to personally identifiable data is provided solely to the authenticated citizens whose identity has been verified at the highest level of verification, as well as to staff with appropriate levels of security clearance and whose role justifies such access.
- Access to pseudonymised data is available by authorised users developing Management Information features and providing technical support.
- Personally identifiable data is shared with relevant care providers such as clinicians who have a legitimate relationship with the patient. Anonymous data may be disseminated and shared in the future with downstream systems such as ONS (The Office for National Statistics) or any other institutions responsible for publishing national statistics or research on healthcare.
- As explained in more detail in the Security section (below), all data is encrypted at rest and in transit, with strict role-based access controls (RBAC) in place.
- Volumes of data are dependent on two key factors. The first is the number of citizens registered for the NHS account, verified at the highest level of identity proofing, and actively using the NHS App. The second factor is the number of trusts that have been registered to use Wayfinder services. For example, the target coverage is 100% of all acute trusts by end of FY25/26.

- There is also an expectation that the number of transactions will increase manyfold in mid to long term. The existing commercial arrangements include fixed capacity agreements which may need to be reviewed as the traffic volumes go up.
- Data stored for longer periods (in the system's databases) are records comprising NHS Numbers and patient-facing system identifiers. These data allow Wayfinder to locate more detailed care information, such as appointments or referrals, at the time that patients request such information. The more detailed information is cached for the duration of the user-authenticated session to enable better performance and provide a better user experience. Such information typically includes metadata items such as the time and date of an appointment, a specialty, clinic or service name, or the name and location of the care-providing organisation. More detailed examples have been provided earlier in Table 3.
- The geographical areas covered include England and the Isle of Man.

Reporting service

The table below describes the key data items forwarded to the Wayfinder Reporting Service by the source systems. The list is not an exhaustive one, however, no additional PID items will be added in the future.

The acronyms used in the table are:

- AGG – Patient Care Aggregator
- REP – Reporting Service
- PFS – Patient Facing SystemAPP – NHS App

Table 4. Data items in the MI events

Description	***Source***	***Destination***	***Data items***
Management Information data	PFS AGG APP	REP	Event Code Timestamp Id NHS Number (Pseudonymised) X Correlation Id (Clear) TrackingId StartDate EndDate Expiry Device GP Preference Old Value New Value Appointment Date / TCIDate EncounterClass ODS Code Status Session Id Appointment Id SpecialtyCode Document Date

			Document Id DocumentType Questionnaire Date Questionnaire Id QuestionnaireType Type PathwayId Entity Id Notification Type Notification Id NewAppointmentId – for reschedule event only Reason – for reschedule event only

Information Flow

Patient Care Aggregator

Appointments, Referrals, Documents, Questionnaires and Wait Times

Error! Reference source not found. demonstrates the end-to-end synchronous information flow. This flow describes the stages and operations of the workflow enabling the patient to receive the needed information in near-real time in response to their request in the NHS App.

Again, outside the scope of this document are the data exchanges between NHS Trusts and their patient-facing systems.

The stages and operations of the information flow, as enumerated in the diagram, are shown in Table 5.

It should be noted that the solution architecture for the Wayfinder service is using a 'stateless' pattern due to the constraints implied by the current set of Directions. A stateless mode of operation means that no appointment, referral, document or questionnaire data is persisted within the system. Therefore, almost every time that the user/patient navigates to a different page/screen, all these data have to be retrieved through API calls again.

The new Directions should allow temporary retention (caching) of the retrieved data to enable a service that is more performant and less costly and one that would at the same time significantly improve the user experience. The retained data will contain personally identifiable information (PII) and will be retained only for the duration of the authenticated user session.

Table 5. Synchronous information flow

Stage	Operation
1	NHS App sends a request to the Aggregator to retrieve appointment and referral data on behalf of the patient using the patient's NHS number
2	The Aggregator's Event Service calls the Aggregator's Record Service to find out which patient-facing systems hold appointments for that NHS Number

3	Event Service requests appointment & referral data from relevant Trust /patient-facing systems, and NHS England systems
4	Trust patient-facing systems and NHS England systems return appointment and referral data, or error messages in case no data could be retrieved.
5	The Event Service resolves ODS codes received from patient-facing systems or NHS England system service IDs into organisation names or service names, through look-ups in the local ODS cache, or by calling the ODS APIs in case no entry was found in the cache, and by calling the NHS directory services, respectively. In case of referrals, the Event Service also retrieves personalised wait times from the waiting time APIs in the context of a specific referral and the patient.
6	Received data gets transformed into relevant internal data structures
7	All received appointment and referral data, as well as error messages, are aggregated into a data 'bundle'
8	As a final step before data are sent to the NHS App, business rules are applied to filter out specific data items
9	Appointment and referral data are returned to the NHS App (and the patient)
10	Hand-off to patient-facing system via a deep link providing patients with access to a richer set of features such as enabling them to manage appointments, view and download documents, complete questionnaires, etc.

Record Locators

Figure 3 (a section of the diagram in Figure 1 or **Error! Reference source not found.**) describes the asynchronous information flow between patient-facing systems and the Patient Care Aggregator. This is a flow of data that happens in the background, independently of the patients' requests to retrieve their data.

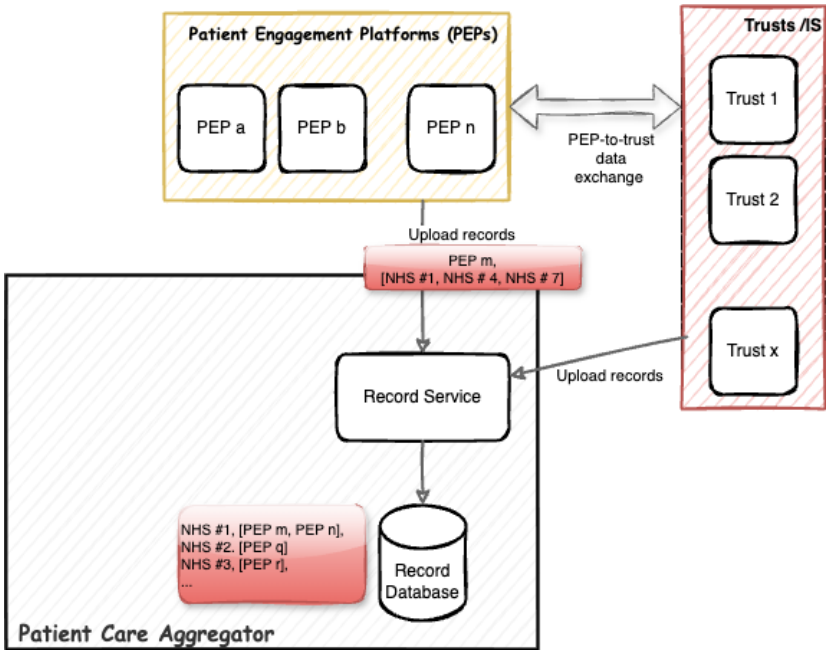

Figure 3. Upload of records

As and when a Trust, patient-facing, or NHS system receives new or updated appointment, document or questionnaire data from a Trust's Patient Administration System (PAS), a notification message is sent to the Record Service in the Patient Care Aggregator. The message contains the patient-facing system identifier and one or more NHS Numbers of citizens who have pending appointments. These 'pointers' to data are stored in the Record Database serving as the *record locators* to be used later (during synchronous information flow, shown as Stage 2 in **Error! Reference source not found.** and Table 5) when requests are made by NHS App to retrieve patients' appointments and related artefacts (such as document or questionnaires).

This upload of records is carried out asynchronously, on a schedule that is managed by each integrated system.

Bypass Mode of Operation

In the event of being unable to retrieve records from the Record Database (shown as step 2 in **Error! Reference source not found.** and Table 5), the Patient Care Aggregator can be switched into a so-called *Bypass Mode* of operation. This scenario can arise from events such as data corruption, Record Database becoming unavailable, or loss of connectivity between the Event Service and the database (see **Error! Reference source not found.**).

In Bypass Mode, the business logic of the Patient Care Aggregator component does not try to get records from the Record Service database to find out which systems hold (appointment, document, or questionnaire) data for a specific NHS Number to send API requests to those particular patient-facing systems (step 3a in **Error! Reference source not found.** and Table 5). Instead, it sends API requests to *all* onboarded patient-facing / Trust systems.

As a result, integrated systems will receive API requests containing PII (NHS Number and other information included in the NHS login's ID token) of patients who do not currently receive care at the trusts serviced by those patient-facing systems. All patient-facing systems have confirmed their IG and product legal teams' agreement with the proposed use of the Record Service Bypass Mode of operation to ensure Business Continuity as a contingency option only, should a Live Service incident require it.

In the event of receiving an API request for an NHS Number that cannot be matched in their databases, patient-facing systems will respond with an error code and discard (delete) any PII received in the API request.

Reporting Service

The data flow is shown in Figure 2.

Outputs of the Reporting Service are consumed by NHSE only. There will be no onward dissemination of outputs to other organisations.

National Elective Waiting List and Contact Service (NEWLICS)

The data flow is shown in Figure 4.

Reference Data Service

The Reference Data Service matches the ODS code to a patient readable trust name.

Security

Patient Care Aggregator

All data in transit (API calls) are encrypted using the industry-standard HTTPS protocol.

All data at rest (the Record Database and the ODS cache) are encrypted using 256-bit Advanced Encryption Standard (AES-256) using encryption keys safely stored in the AWS KMS.

Figure 4 shows the authentication controls used in Wayfinder. They are:

- **mTLS** – Mutual Transport Layer Security (mTLS) is a process that establishes an encrypted TLS connection in which both parties use X. 509 digital certificates to authenticate each other.
- **MFA (or, Multi-Factor Authentication)** – an authentication method in which a user is granted access to a service (e.g. website or application) only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism: *knowledge* (something only the user knows), *possession* (something only the user has), and *inherence* (something only the user is).
- **API Key** – a unique identifier used to authenticate a user or calling system to an API
- **OAuth 2.0 Client Credentials Flow** – a grant used to access some server-hosted resources (data) by using the identity of an application. This type of grant is commonly used for server-to-server interactions that must run in the background, without immediate interaction with a user.

The authorisation is achieved by sending the (NHS login's) ID Token in all the API calls to patient-facing systems and e-RS. The receiving systems can decrypt the ID Token (by using the NHS login's public key / digital certificate) and thus verify the user (via the NHS Number contained in the ID Token).

Reporting Service

Access to the anonymised data is currently provided only to authorised users, largely those who are developing and using the Management Information features, as well as the Live Service Support team.

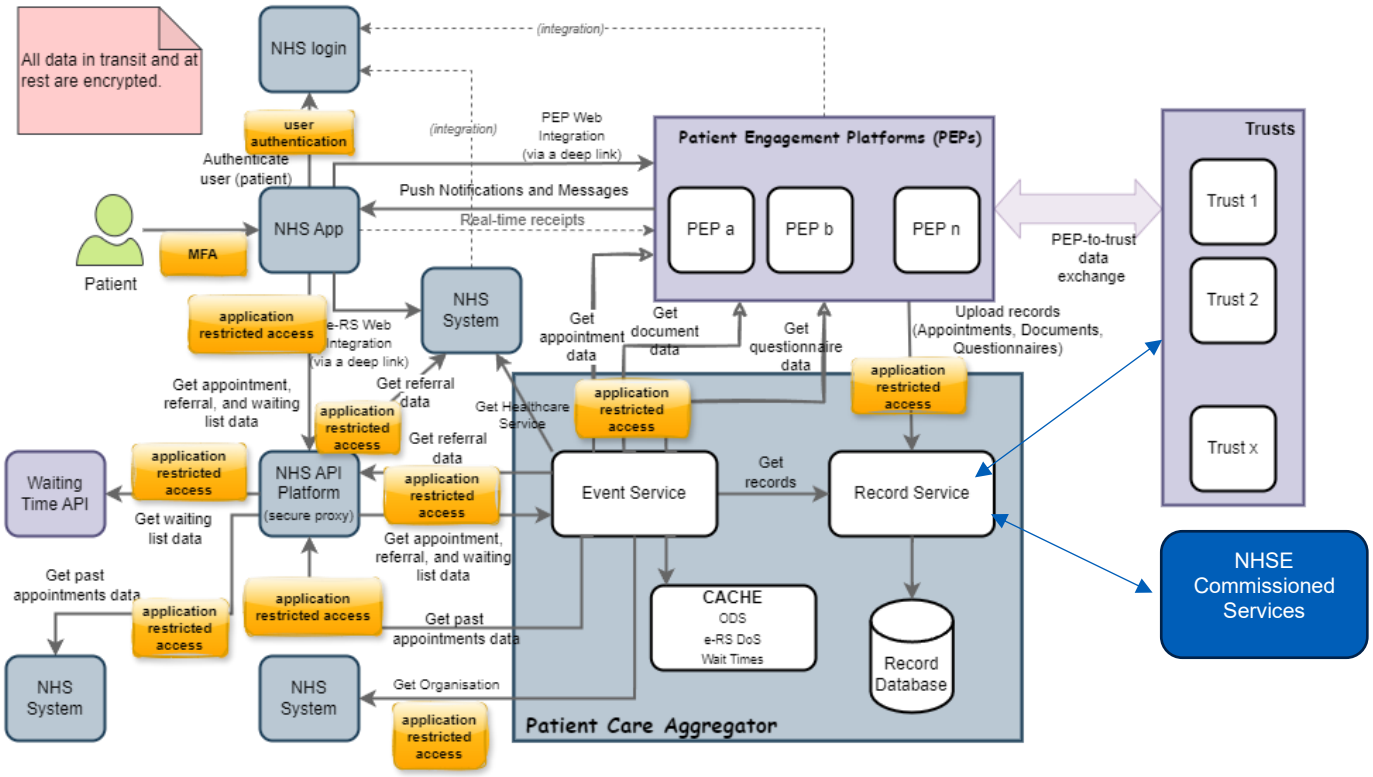

Figure 4. Authentication controls in Wayfinder

It is worth noting that the retrieval of documents and questionnaires does not include the contents of those documents and questionnaires. This is outside the scope of the Wayfinder service which only uses a 'pointer' (i.e. the deep link) sent from the patient-facing / Trust / NHS England Commissioned services (systems) that will resolve the user to a document or questionnaire that is hosted on the patient-facing system.

Waiting List Service

All data in transit (API calls) are encrypted using the industry-standard HTTPS protocol.

All data at rest (the Waiting List Data Store) are encrypted using 256-bit Advanced Encryption Standard (AES-256) using encryption keys safely stored in the AWS KMS.

Figure 47 shows the authentication controls used in Wayfinder. They are:

- **mTLS** – Mutual Transport Layer Security (mTLS) is a process that establishes an encrypted TLS connection in which both parties use X. 509 digital certificates to authenticate each other.
- **MFA (or, Multi-Factor Authentication)** – an authentication method in which a user is granted access to a service (e.g. website or application) only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism: *knowledge* (something only the user knows), *possession* (something only the user has), and *inherence* (something only the user is).
- **API Key** – a unique identifier used to authenticate a user or calling system to an API
- **OAuth 2.0 Client Credentials Flow** – a grant used to access some server-hosted resources (data) by using the identity of an application. This type of grant is commonly

used for server-to-server interactions that must run in the background, without immediate interaction with a user.

The authorisation is achieved by sending the (NHS login's) ID Token in all the API calls. The receiving systems can decrypt the ID Token (by using the NHS login's public key / digital certificate) and thus verify the user (via the NHS Number contained in the ID Token).

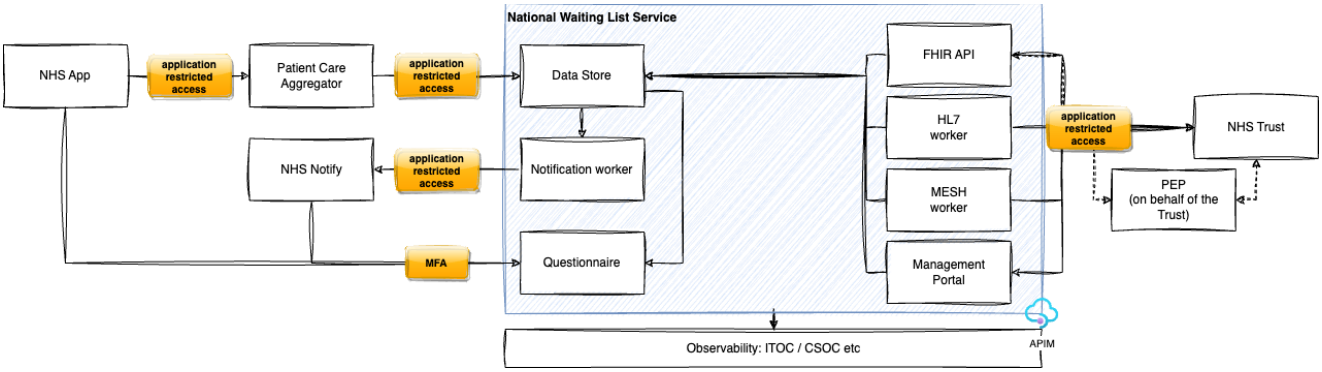

Figure 7. Authentication controls in National Waiting List Service

Reference Data Service

The reference data service is an internal service within the Patient Care Aggregator component. This consumes the Organisational Data Service which is publicly available organisation data and does not contain any sensitive data to secure against.