Secondary Care Appointments via the NHS App

Contents

Brief summary - purpose of service and function

NHS Wayfinder is a programme that will enable NHS Digital to provide a service to NHS patients in England through the NHS App and the NHS website to securely view summary details of their scheduled secondary care appointments with acute NHS Trusts and to enable them to access further details about those appointments from the NHS App. It will present an aggregated view of all outpatient referrals and all secondary care outpatient appointments associated with the user's NHS Number:

- **Referrals:** Directly Bookable, Indirectly Bookable and RAS referrals and their status (Ready to Book, Ready to Rebook, In Review, Review by Clinic Overdue, Booked, Ready to Confirm Appointment, Cancelled).
- **Secondary Care Outpatient Appointments**: Future appointments and their status, including cancelled future appointments.

Referrals and appointments will be sourced via **Application Programme Interface (API) integration** with a new NHS England Patient Care Aggregator. This service processes appointment data from multiple Patient Engagement Portals (providers)[PEPs] and will apply business rules regarding what appointment data will be presented. This will enable users to access (using a deep-link functionality built on existing NHS App and web integrations and reusing NHS login token generated when the user accesses the NHS App. **E-RS** is used to book their initial outpatient appointment, using the existing Manage Your Referral (MYR) synchronous booking functionality. **Patient Engagement Portals** will then facilitate a user to book, change and cancel existing appointments. The aggregation service will be integrated within the NHS Digital (NHS Digital) Organisation data Service (ODS) to validate appointment speciality data presented to the user - **those aged 16 and over.**

Background

In February 2022, NHS England published a 'Delivery Plan for tackling the COVID-19 backlog of elective care'. In this plan 4 commitments were made:

1. Waiting times for elective care of more than 1 year eliminated by March 2025
2. That 95% of patients needing a diagnostic test receive it within six weeks by March 2025
3. By March 2024, 75% of patients urgently referred by their GP for suspected cancer are diagnosed or have cancer ruled out within 28 days
4. For patients who need an outpatient appointment, the time they wait to wait will be significantly reduced by transforming the model of care and making greater use of technology.

For further information, click on the link below.

https://www.england.nhs.uk/2022/02/nhs-publishes-electives-recovery-plan-to-boost-capacity-and-give-power-to-patients/

The Secretary of State and DHSC looked at how our national digital channels of the NHS App and Website could be used to empower patients to book and manage elective care

appointments digitally. A 'Wayfinder' team was set up between NHS England's Transformation Directorate and NHS Digital to apply digital technology and data systems to free up capacity:

Chapter 2(B) Using digital technology and data systems to free up capacity

- Ensuring "that digital technologies that can improve access and flexibility for patients and free up capacity to suit them are scaled across the NHS" (p.18)
- "Improve core digital and data services in hospitals to ensure we have the basics right, as well as harness and scale innovations that have shown high impact in some areas of the country. We also want to use national digital tools such as the NHS App to provide a personalised route into NHS services for patients, making care more convenient and driven by patients' needs." (p.18)

Chapter 4 (C & E) Improving patient pathways to reduce avoidable delays by ensuring we are making the best use of the latest technology, clinical time, and expertise

- "Providing greater flexibility in how advice from clinicians is accessed by patients, enabling more timely, convenient and appropriate care and avoiding the need for unnecessary appointments." (p.31)
- "Giving patients more choice around outpatient care, with options to book their follow-ups and attend video/phone consultations if preferred, simultaneously freeing up capacity for the most clinically urgent. This will include digital innovation through the NHS App."
- "More flexible follow-ups – giving patients and their carers the flexibility to arrange their follow-up appointments as and when they need them. The approach helps empower patients to manage their own condition and plays a key role in enabling shared decision-making and supported self-management."

Chapter 5 Better information and support for patients

- "Create a transparent, well-informed process for service users that complements existing local communication channels between the health system and patients." (p.41)
- "Series of linked interventions, coalescing around a central platform that will host the information for patients (NHS App)." (p.41)
- "We will develop guidance to support local health systems to provide personalised and targeted support for patients and their carers to help them manage their symptoms while they wait, prevent deterioration and recover effectively." (p.43)

And also, as part of the NHS Long Term Plan:

Providing action to ensure patients get the care they need, fast. (Chapter 1)
By being able to access information about waiting times, see and manage appointments and access advice about how to manage their condition people will be provided with:

- More control over their own health and more personalised care when they need it

What is 'Wayfinder'?

Wayfinder will deliver functionality to the NHS App to support patients waiting for care/elective recovery. The programme is leveraging the innovative work being delivered at many NHS acute trusts through Patient Engagement Portals (PEPs). Patient Engagement

Portals are NHS partners who deliver a wide variety of capabilities to patients and clinicians. They allow patients to access information about their care in a secure online setting. Many currently provide the ability to book appointments, answer pre-consultation questionnaires and to communicate directly with clinicians. Working with these partners allows Wayfinder to combine local innovations with the national reach of the NHS App to deliver digital transformation for patients and the NHS across England.

The programme is intended to enable the NHS to deliver against several policies and strategies for the benefit of elective care services, patients, and their carers. By increasing the functionality of the NHS App (on the heels of the success of the NHS COVID Pass, used by approximately 30 million users), digitally enabled care can become mainstream. It is hoped that providing better information and support to patients will reduce the number of missed appointments as well as being a more personalised and convenient route to see their data.

The user journey will start with NHS login, verifying patients at the highest level of authentication (P9). This will allow a patient to gain access to the NHS App for a variety of approved connected services as well as viewing e-Referral Service (e-RS) referrals and NHS Trust hospital appointments.

Appointment and referral data will be provided by an 'Aggregator' application which surfaces information from e-RS and integrated Patient Engagement Portals. It links that data to information held by NHS Digital's systems. The Aggregator is being built by a 3rd party company - Servita - and set up within the NHS Digital environment.

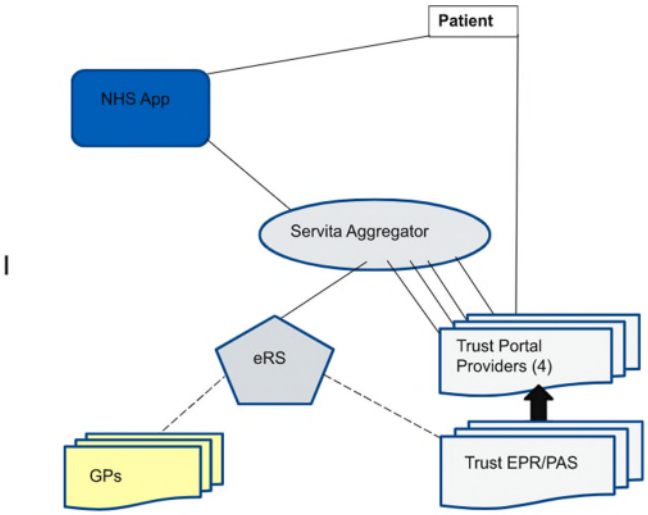
When a patient views their referrals and appointments, they may select to launch into deeper features provided by e-RS and Patient Engagement Portal (PEP) systems. These features include booking, amendment or cancellation of appointments, surfacing of related documents and relevant contact details for their Hospital as a single point of contact.

Further enhancement to support patients on a waiting list will be added in due course.

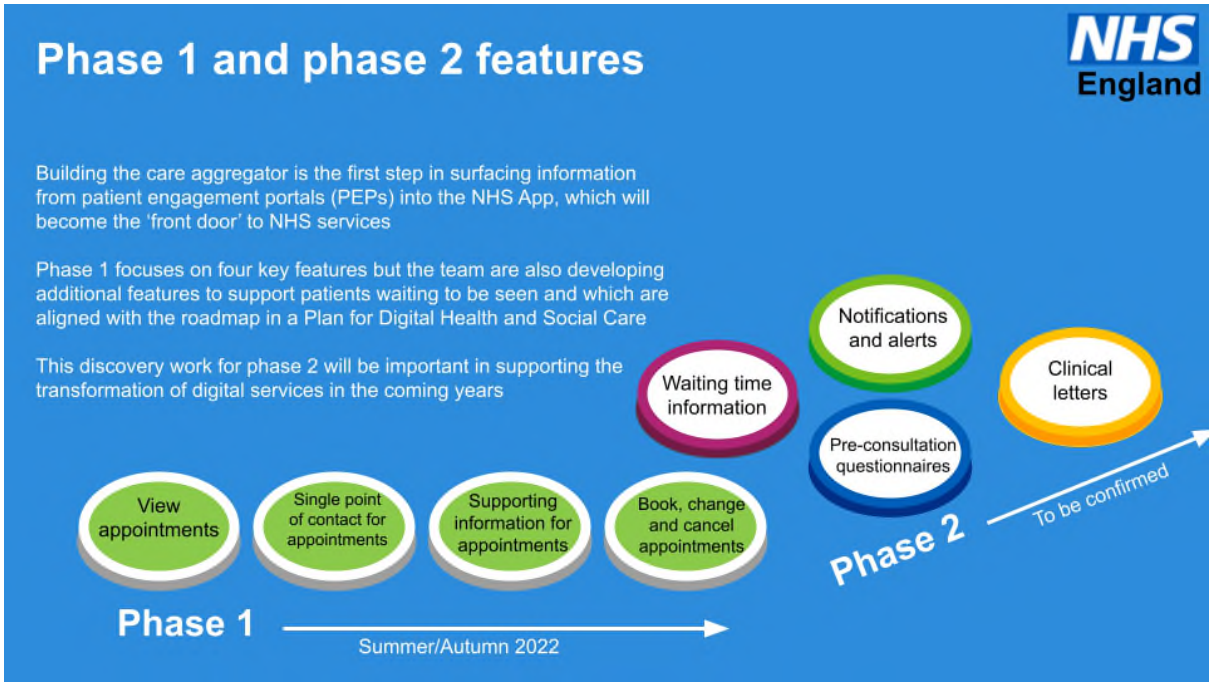
Useful definitions are: -

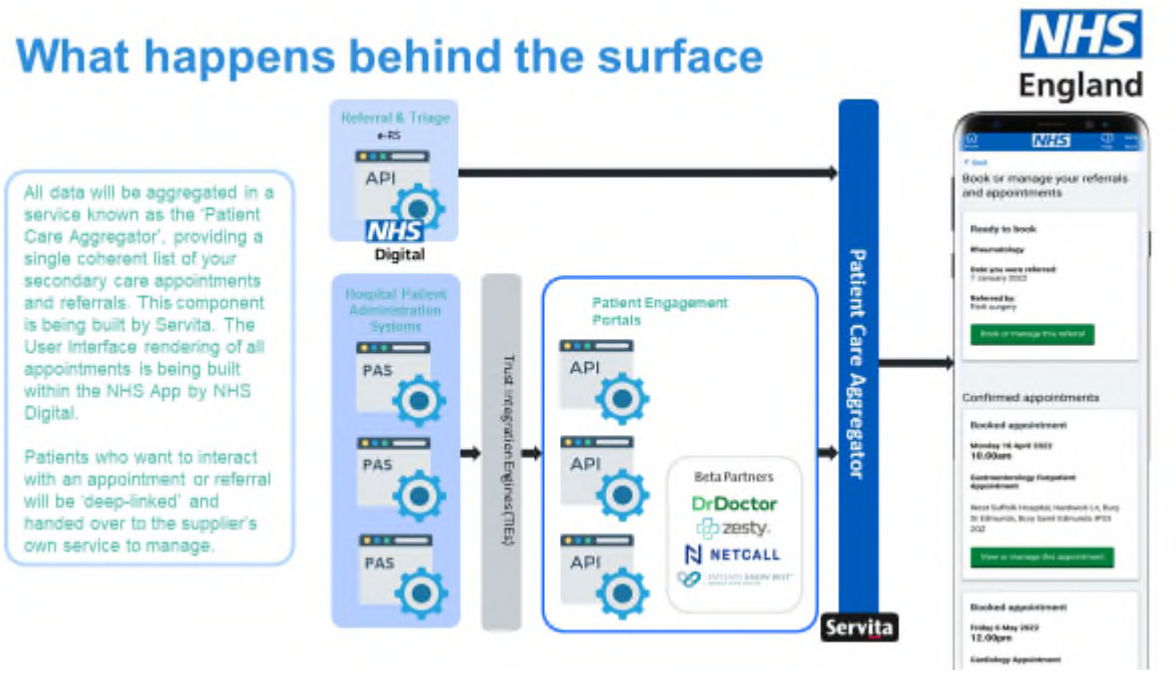
- **Wayfinder** is the programme delivering functionality to allow patients to access and manage secondary care appointments and referrals through the NHS App

- **Patient Care Aggregator** is a core application which enables Wayfinder to deliver target features, it aggregates data from several sources and renders it to patients in a single, coherent list.



- **Beta** phase initial launch Summer 2022, Smoke testing in the Trust to commence 12th September and rollout of the beta phase if successful 20th September 2022





Phase 1 go-live in Sherwood Forest Hospitals

There are 4 features that are part of the Phase 1 go-live (also known as the smoke test process) scheduled for deployment 12th September 2022:

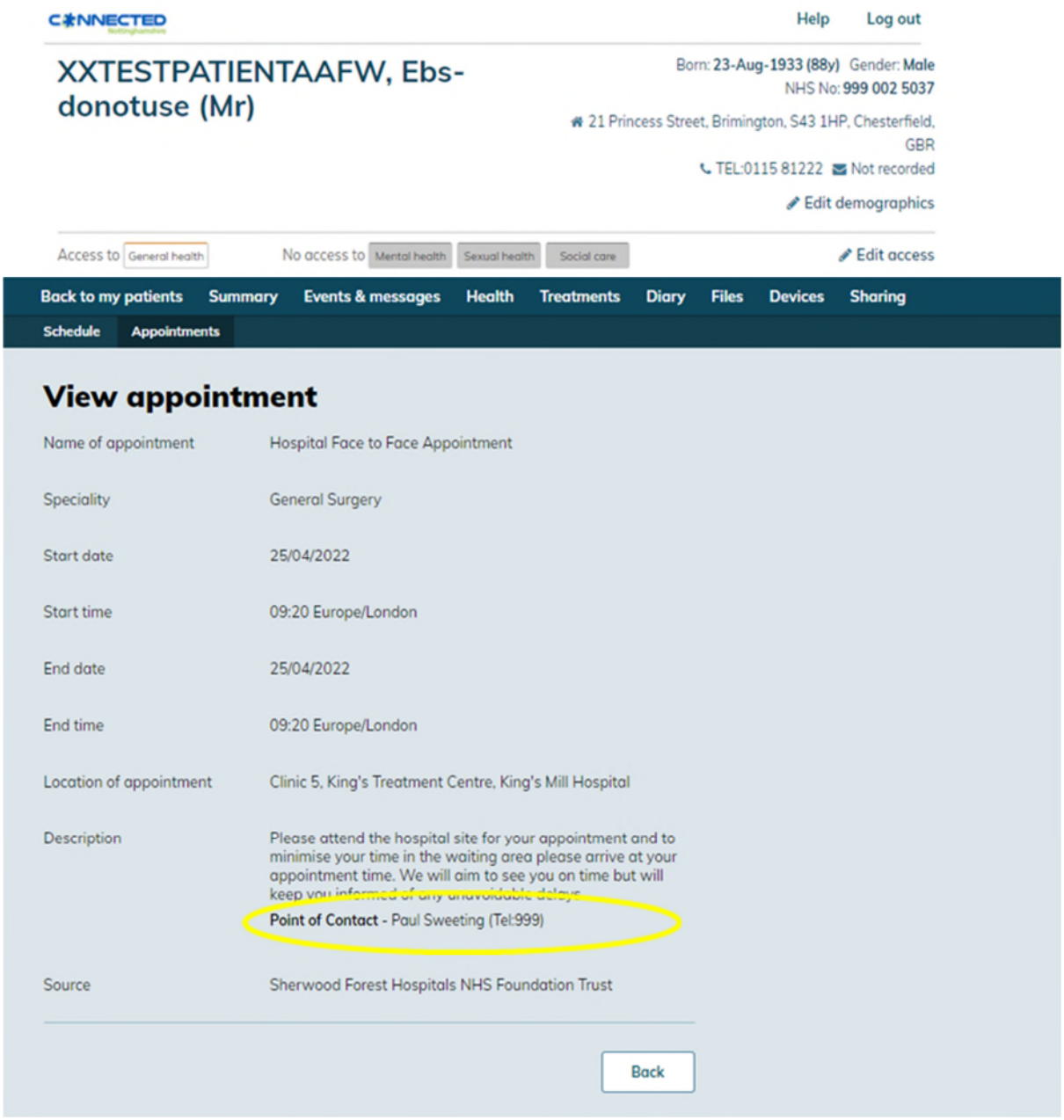
We will be implementing these as follows:

1. **View appointments**: The Trust already has a HL7[1] feed taking all outpatient appointment information from CareFlow EPR into Patients Know Best (PKB). Radiology appointments are not booked on CareFlow EPR and not currently part of the HL7 feed. However Radiology appointments will be made available in the NHS App once the technical mechanisms and HL7 feeds are available.

[1] HL7 - Health Level Seven® International (HL7®) is the global authority on standards for interoperability of health technology and is the global industry standard for passing healthcare data between systems. The data is transmitted via HL7 and encrypted both in transit and at rest.

2. **Access to relevant resource**: The Trust has engaged in discussions with the NHS Wayfinder Team, and data/information for this functionality will be available on My Planned Care NHS. No further action is required from the Trust.

3. **Provide a single point of contact**: The Trust will include our Booking Team's phone number and email address, within the description of the appointment as below:



4. **Appointment Management**: Similar to displaying a point of contact with the appointment details, as described above, we will be adding information notifying the patient to use those details (Booking Team's phone number or email address) should they need to make any changes to their appointment.

Patients Know Best (PKB) have developed functionality to enable Appointment Management which makes use of their messaging functionality. We are not implementing this at this stage but plan to utilise the functionality at a later date.

Onboarding patients to Wayfinder

Sherwood Forest Hospitals NHS Foundation Trust has a contract in place with Patients Know Best as a Patient Engagement Portal (PEP) and we have both agreed to take part in 'Wayfinder'.

The Patient Engagement Portal (PEP)'s list of NHS numbers is made available by a one-off bulk upload from that Patient Engagement Portal (PEP) to the Wayfinder Records Service (store) of the Patient Care Aggregator, except where the Trust, by instruction to the Patient Engagement Portal (PEP) has excluded certain data (e.g., specialist clinics) by maintaining their own Excluded Patient Lists. The data types collected and stored in the Records Service (ready to enable a live service interaction with the Wayfinder Appointment Events Service part of the Care Aggregator), are a patient's:

- NHS Number
- Patient Engagement Portal (PEP) unique ID

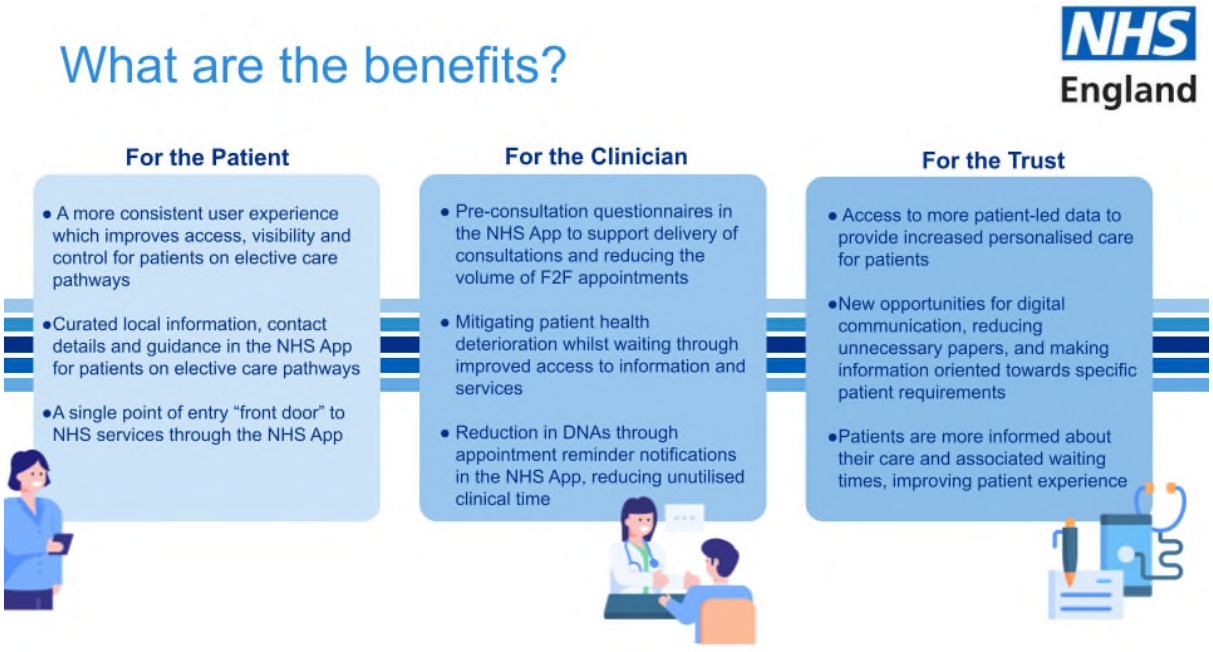
The bulk uploaded data is subsequently updated periodically with data from the Patient Engagement Portal (PEP) to ensure the Records Service store is kept up to date.

Benefits associated with patients, society, service, cost, and productivity

- Communications to patients can be in one place - avoiding paper copies
- The use of the NHS App will attract larger numbers of users nationally as the coverage is rolled out and gain more users than a local option alone
- Providing up-to-date information in a reliable format allows patients to feel comfortable they are being informed
- Communicating changes is simplified and clearer
- Prevents the inconvenience and anxiety of having to chase up on what stage something is at
- A reduction in costs associated with acute trusts' communications with patients via SMS messaging.
- People are now familiar with the NHS App and trust this way of sharing data as a live feed
- Introduces flexibility for the patient that allows them to work around their own lifestyles and commitments.
- Provides a clear, single point of contact for patients
- The ability to access relevant resources whilst waiting for care (with an ongoing potential for development into areas like outcome letters, alerts, and notifications about appointments, pre-consultation questionnaires).
- Drive participatory health
- Working with current systems and healthcare providers
- Embracing the innovation, learning and development that has taken place locally to

apply nationally.

- Reduce or remove the patient journey pain points - visualise progress, keep people engaged, explain the wait, and avoid uncertainty
- An overall improvement in patients' experience of accessing secondary care services, as a result of improved level of available appointment information and the ability for patients to select their appointment at a time that is convenient for them.
- A reduction in costs associated with acute trusts' communications with patients via SMS messaging.
- A reduction in the financial impact of 'Did Not Attend' (DNAs), resulting from patients' ability to select, view, change, and cancel their appointment times through the NHS App.
- A reduced financial impact caused by on-day cancellations.
- A reduction in waiting times through better utilisation of clinics, a lesser degree of waste in the system, and efficiencies driven through freed up administrative time and a reduction in DNAs.
- A smaller carbon footprint because of a reduced need for printing.
- Offering potential for innovation including condition specific guidance while on a waiting list and to promote wellness where possible with promotion of awareness for supporting services.



What is the NHS Patient Care Aggregator?

The NHS Care Aggregator is comprised of two parts –

1. **the Records Service** (data set of NHS number and client ID determining the identity of the PEP) and
2. **the Events Service** (data set comprising all secondary care appointment information of a patient – date, time, location, type, status etc)

The Records Service is populated by data from each NHS Trust via their PEP. The data set that is both collected and stored by NHS England as data controller for the Care Aggregator, is the **NHS number and client ID for the PEP itself**. This is initially enacted as a bulk upload, refreshed periodically to maintain data accuracy and completeness.

For the Events Service, the secondary care appointment landscape is variable from NHS Trust to Trust and by differing formats. When a patient engages with the NHS App appointments tab to see their data, this action triggers a request to a PEP, taking milliseconds in real time. A filtering process takes place based on Care Aggregator business rules, to establish if that patient has any secondary care appointments with a Patient Engagement Portal (PEP). Filtering makes use of ODS codes of the Trust and their cohort of GP practices.

Simultaneously, the patient's NHS login ID Token is passed forward to the Patient Engagement Portal (PEP) to request, match and validate the user against appointment data located with a Patient Engagement Portal (PEP). The business rules filter out NHS Trusts that are not in the programme. Any rejected data is automatically deleted in the same immediate timeframe.

The Events Service data set comprises speciality of appointment, time, date, booking status, type and when last updated by system.

Unlike the Records Service, data is not of a bulk upload nature, and is not collected or stored within the Care Aggregator. Instead, it generates a display to the user within their NHS App as a live feed.

The user journeys

1. NHS login (identity verification):

Beginning with authentication, this is a service that has been created by the NHS for patients and the public. It provides a re-usable way for patients to access multiple digital health and social care services with a single login, which includes authentication for returning users. The highest level of verification is provided for a patient to be able to have sight of their hospital appointments from within the NHS App. This is called P9, based upon DCB3051 Identity Verification and Authentication Standard for Digital Health and Care Services

https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/dcb3051-identity-verification-and-authentication-standard-for-digital-health-and-care-services

More detail on NHS login is available here: https://digital.nhs.uk/services/nhs-login/

2. NHS App:

The NHS App has 2 integration patterns - web based (via nhs.uk) and the NHS App. For the Wayfinder Programme, we will only be using an Application Programme Interface (API) based integration pattern into the NHS App. This is a mobile app allowing access to a patients NHS account (technically NHS App refers to the application, but an NHS account can also be accessed through the NHS website). The NHS App provides a range of services to people aged 13 or over who are registered with an NHS GP surgery in England. Although those aged 13 can access the NHS App with suitable verification, the secondary care appointments service will only be available to those aged 16 and over. The NHS App offers a range of functionality, allowing users to get a Covid pass, order repeat prescriptions, etc. From the secondary appointments display perspective, there is no collection of personal data from the patient other than service monitoring/data quality.
More detail is available here: https://digital.nhs.uk/services/nhs-app

3. NHS e-Referral Service:

The NHS e-Referral Service (e-RS) is a programme under the data controllership of NHS Digital (in relation to the processing of personal data) and the Department of Health and Social Care (DHSC) (in relation to determining the purpose for processing the data through the issuing of a direction to NHS Digital). This service provides an easy way for patients to choose their first hospital or clinic appointment with a specialist. Bookings can be made online, using the telephone, or directly in the GP surgery at the time of referral.
This system electronically captures GP (and other clinical) referrals from a primary care environment and enables a referral process that engages with NHS Trusts in the secondary care environment. The digital platform is fully integrated into NHS Trust clinical systems and captures the referral and **first appointment** following the referral. In 2018, there was a national drive to increase e-RS adoption via the 'paper switch off' programme by ceasing secondary care payments for all referrals not received electronically via the e-RS platform. This resulted in high utilisation of e-RS for primary care referrals. 'Manage Your Referral' is the patient facing website that allows users to book, rearrange and cancel their referral/first appointment online as well as providing an overview of the status of referral. For further privacy information, go to

https://digital.nhs.uk/services/e-referral-service/document-library/privacy-statement---nhs-e-referral-service

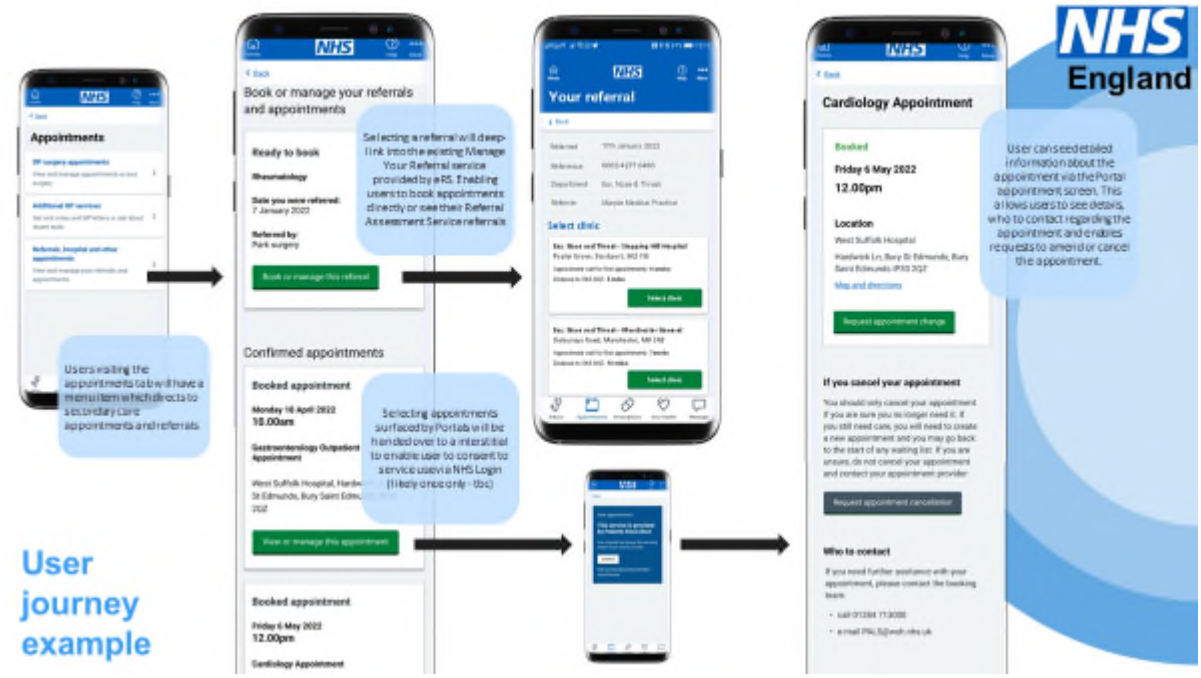
The aggregator simultaneously asks e-RS and the portals for appointment information associated with the patient. Once this is received, the aggregator has a set of rules that it uses to filter out appointment information that either shouldn't be shown to the patient or any duplicates.

There are business rules in place, fulfilled by the Aggregator that addresses potential duplication:

1. Where information is provided by both e-RS and a Patient Engagement Portal (PEP) system for the same appointment, the e-RS version will be shown to the user

2. Where a trust uses two Patient Engagement Portal (PEP)s, one has been selected as the master for appointments management. If appointment information is received from the 'secondary' Patient Engagement Portal (PEP), it will not be shown to the user
3. Referrals that have already been booked are filtered out, so there is no old referral being shown where the user should instead be looking at the appointment

An illustration of a user journey is as below:



More detail is available here: https://digital.nhs.uk/services/e-referral-service

In summary, e-RS will return the following to the Patient Care Aggregator on request:
- All directly bookable and RAS referrals including their status
- All booked e-RS appointments including time, date, and location
- A direct link to e-RS referral for all booking types

4. Patient Engagement Portals (PEPs or PPs - Portal providers)

Local NHS Trusts manage their patient data on their own digital Patient Administration Systems (PAS). They are free to engage suitably assured Patient Engagement Portals (PEPs), also referred to as Portal providers (PPs). These systems hold all appointments from a provider's (NHS Trust) clinical systems, with the exception of certain types of sensitive or 'S' flagged data. Each system will have mechanisms for features including bookings, messaging, pre and post clinical assessment and clinic scheduling. All appointments scheduled via e-RS will be located within the respective Portal Providers for that provider. Many NHS Trusts are offering their patients digital web-based access to their secondary care appointments via their respective Portal Providers. If a patient receives care through multiple providers, they have to access multiple Portal Providers with varying functionality to piece together and understand their elective care pathway.

An illustration of the MVP is on the next slide as below:

In summary, the Patient Engagement Portal (PEP) systems will

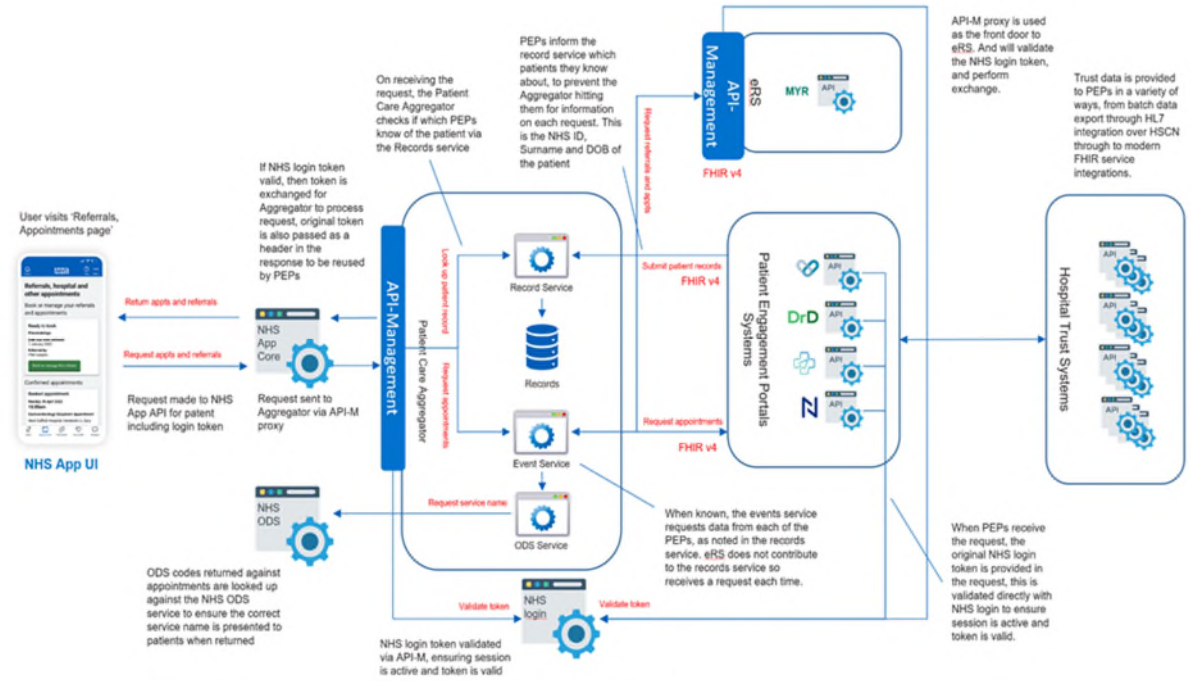
- Validate user access to their portals using NHS Login
- Return the following to the Patient Care Aggregator on request:

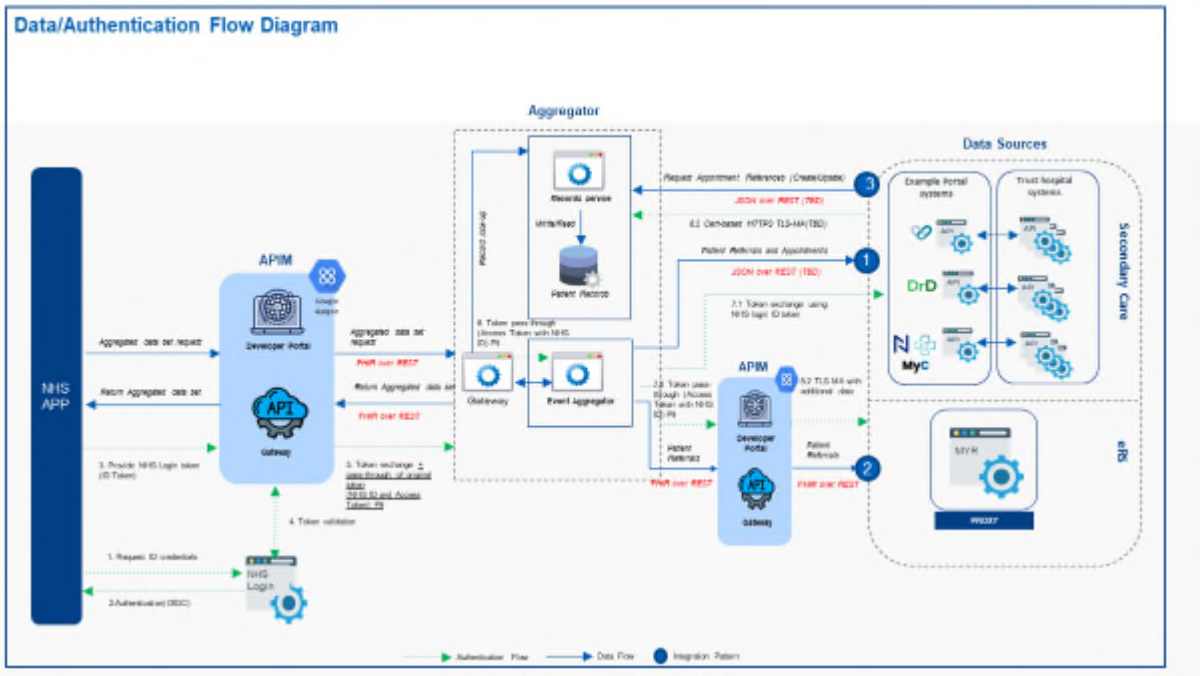
o All patient secondary care appointment information
o Direct links to all appointments

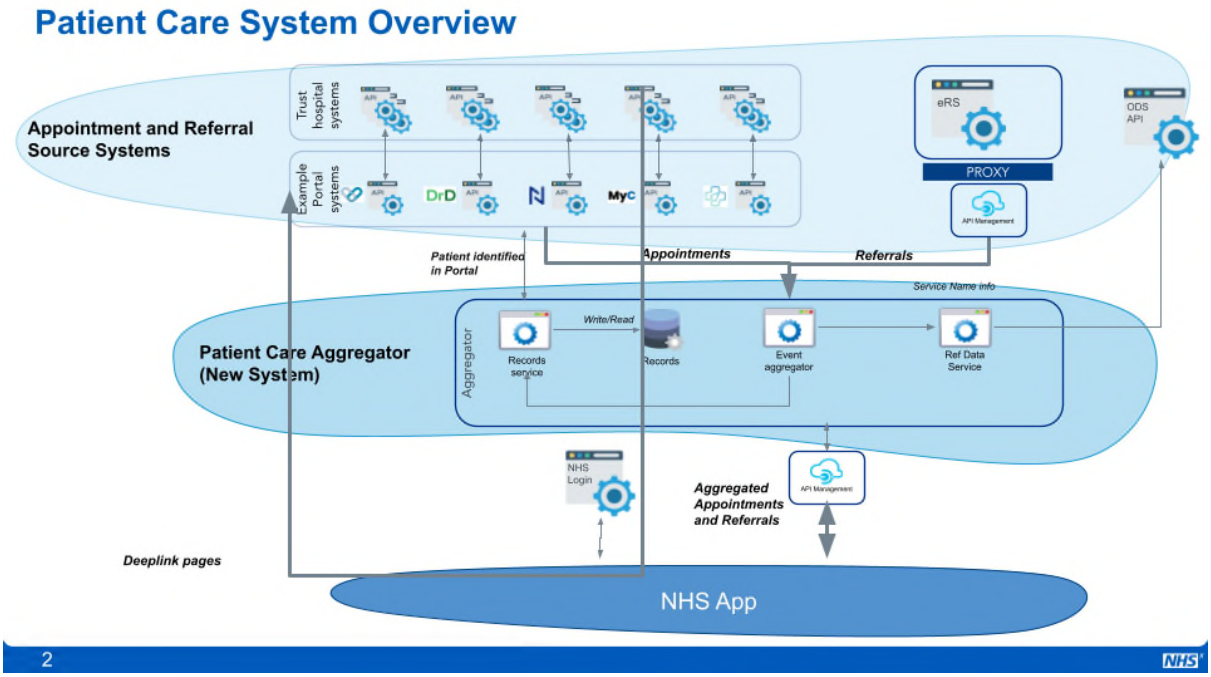
- Enable patients to book, change or cancel their appointments
- Provide a user interface that aligns with NHS App requirements
- Limit patient data to England Trusts only and filter sensitive and ghost appointments
- Provide a single point of contact and locally curated appointment support content to users

Data flows

The end-to-end journey data flow is represented in the following 2 slides:


User visits 'Referrals, Appointments page'
NHS App UI
Return appts and referrals
Request appts and referrals
NHS App Core
Request made to NHS App API for patent including login token
If NHS login token valid, then token is exchanged for Aggregator to process request, original token is also passed as a header in the response to be reused by PEPs
Request sent to Aggregator via API-M proxy
API-Management
Patient Care Aggregator
On receiving the request, the Patient Care Aggregator checks if which PEPs know of the patient via the Records service
Look up patient record
Request appointments
Record Service
Records
Event Service
ODS Service
Request service name
NHS ODS
ODS codes returned against appointments are looked up against the NHS ODS service to ensure the correct service name is presented to patients when returned
PEPs inform the record service which patients they know about, to prevent the Aggregator hitting them for information on each request. This is the NHS ID, Surname and DOB of the patient
Request referrals and appts
API-Management
eRS
MYR
FHIR v4
Submit patient records
FHIR v4
Request appointments
FHIR v4
Patient Engagement Portals Systems
DrD
When known, the events service requests data from each of the PEPs, as noted in the records service. eRS does not contribute to the records service so receives a request each time.
API-M proxy is used as the front door to eRS. And will validate the NHS login token, and perform exchange.
Trust data is provided to PEPs in a variety of ways, from batch data export through HL7 integration over HSCN through to modern FHIR service integrations.
Hospital Trust Systems
When PEPs receive the request, the original NHS login token is provided in the request, this is validated directly with NHS login to ensure session is active and token is valid.
Validate token
NHS login
Validate token
NHS login token validated via API-M, ensuring session is active and token is valid

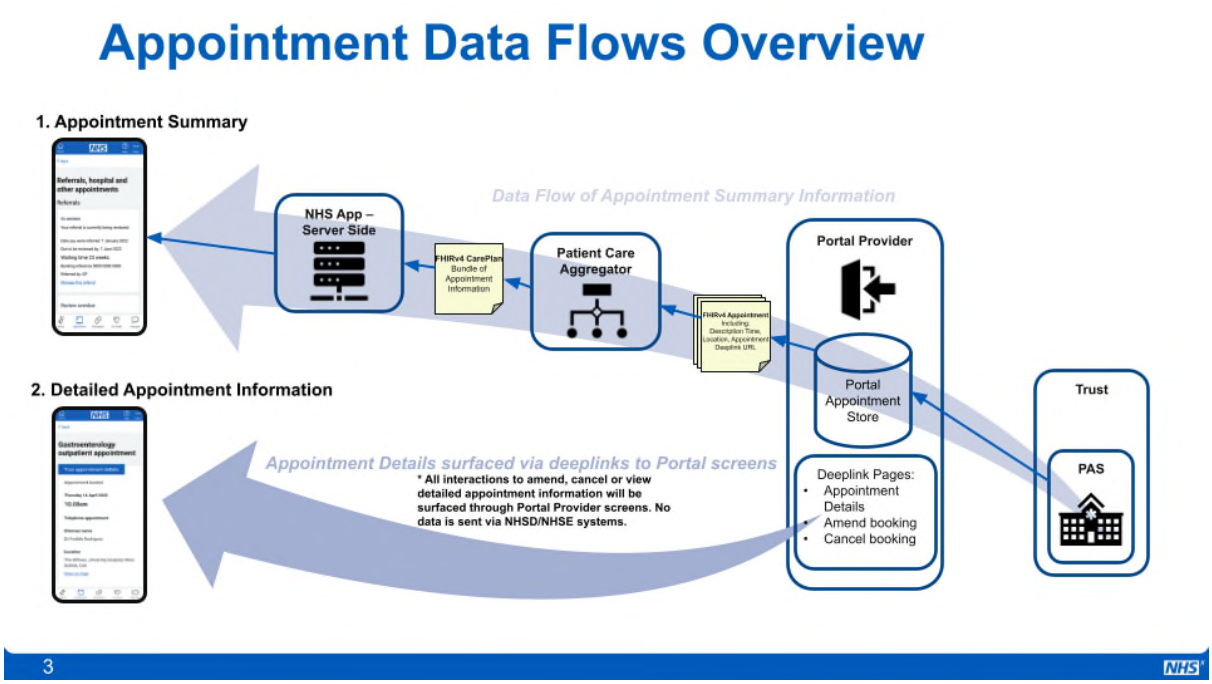

Data/Authentication Flow Diagram
Aggregator
Data Sources
NHS APP
APIM
Developer Portal
API
Gateway
NHS Login
Aggregated data set request
Return Aggregated data set
Records service
Patient Records
Gateway
Event Aggregator
APIM
Developer Portal
Gateway
Example Portal systems
Trust hospital systems
DrD
MyC
Secondary Care
eRS
MYR
Authentication Flow
Data Flow
Integration Pattern



There are 3 data flows required to enable e-RS and local NHS Trusts data to provide a live feed to the patient within their NHS App:

1. **Summary appointment information data flow**. This flow is enacted when a patient in the NHS App requests to view their Secondary Care appointments and referrals. At this point a request is sent from the NHS App to the Patient Care Aggregator. The Aggregator then sends a request to the relevant Application Programme Interface (API) exposed at a Portal Provider and requests all future appointment information for the patient to be provided. The Portal Provider sends an agreed set of appointment summary information that can be displayed on an appointment card in the NHS App, which is enough to allow the patient to identify the appointment. This includes the appointment description, time, and location. The Aggregator then receives this information and processes it against a defined set of business rules before providing details of all appointments and referrals back to the NHS App to display.

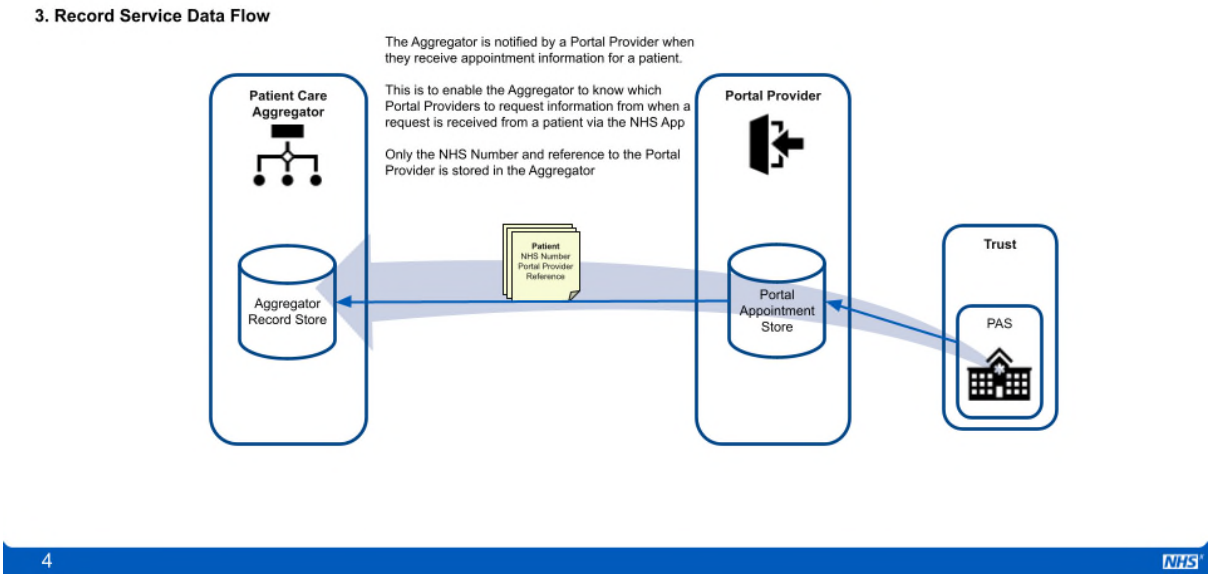
2. **Detailed appointment information data flow**. This flow is where a patient viewing appointment summary information in the NHS App can then request to see more detailed appointment information and complete actions to request an appointment amendment or cancellation. When the patient clicks to view a specific appointment's detail, they are sent via a deep link to a screen served from the Portal Provider. All interactions from this point are to deep link screens served from the Portal Provider and therefore no data is sent from the Portal Provider via the Aggregator. The Portal Provider will supply deep link screens that will allow the patient to understand and manage their appointment, using functionality and processes that they apply through their standard portal screens. The difference will be that the screens will be viewed via the NHS App and apply user interface designs to align with this.



3. **Record service data flow**. This flow is needed to enable the Patient Care Aggregator to know which Portal providers need to be contacted to provide appointment information for a specific patient. The Portal Providers follows data minimisation principles as instructed by their NHS Trusts, for every patient that has a record in the PAS system. National Data opt Outs do not apply to direct care data. This list of patients includes those with an appointment (removed when no longer required). When in real time, a patient seeks their in-app appointment details, a request is sent from the NHS App to the Aggregator via an Application Programme Interface (API). This allows data to be surfaced from both e-RS and Patient Engagement Portal (PEP)s where there is an appointment. To enable this a Portal Provider shall send only the NHS Number for a patient which they have received appointment information for from a trust. The Aggregator will store the NHS Number for each patient with a reference to which Portal Provider they have appointment information stored within. When a patient requests to view an appointment from the NHS App, the Aggregator will check its Record Store and find out which Portal providers to send a request to for appointment summary information. An Application Programme Interface (API) call to the relevant Portal Provider service will be made and information received via data flow. Those users who want to view, book, amend or cancel their appointments require that they leave the confines of the NHS App into the relevant systems holding the data and which can manage this digitally and locally. NHS Trusts are mapped out to GP ODS codes.

   See slide below:

Record Service Data Flow Overview



Aggregator to e-RS integration. E-RS uses an Application Programme Interface (API) to allow data to be surfaced in the Aggregator

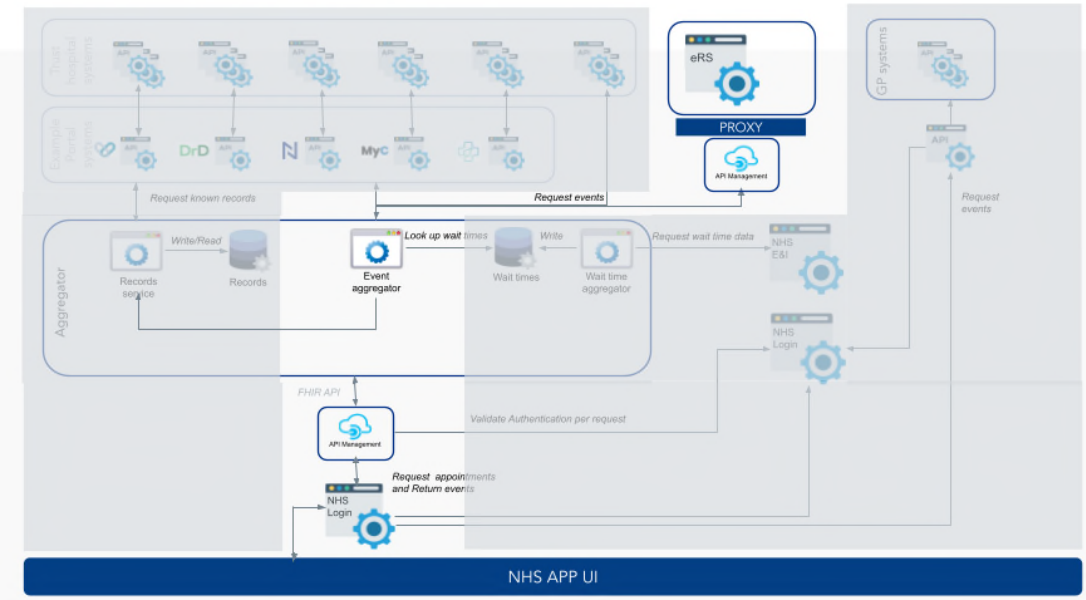
An Aggregator pulls content based on relevant keywords and displays in a curated format. An Application Programme Interface (API) is a software intermediary that allows applications to talk to one another. When the Aggregator has a complete list, each component item will include a URL (Uniform Resource Locator) provided either by e-RS or a Portal Provider for each object (patient) returned. This URL can be launched to provide a pass-through to services wherein a user can perform interactions. This includes amendment and cancellation of appointments and the surfacing of data such as the patient's single point of contact.

The Aggregator will:

- First call the Referrals Application Programme Interface (API) via the e-RS Proxy in Application Programme Interface (API). There will be one call per user/patient request from the NHS App with the NHS number being passed as the identifier.
- Following referral information being returned the Service Application Programme Interface (API) may be called multiple times, with one call per health care service which a referral is linked to.
- The Aggregator is owned by NHS England. 1st line & 2nd line live services support will be provided by NHS Digital and 3rd line support will be provided by NHS England

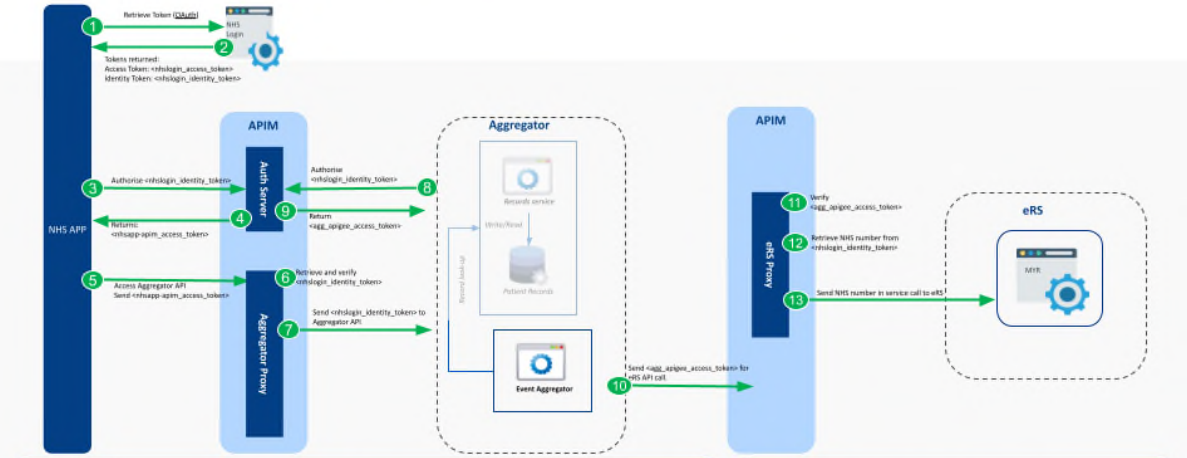
The following 3 slides provide the data flow journey

Aggregator to eRS Integration



7

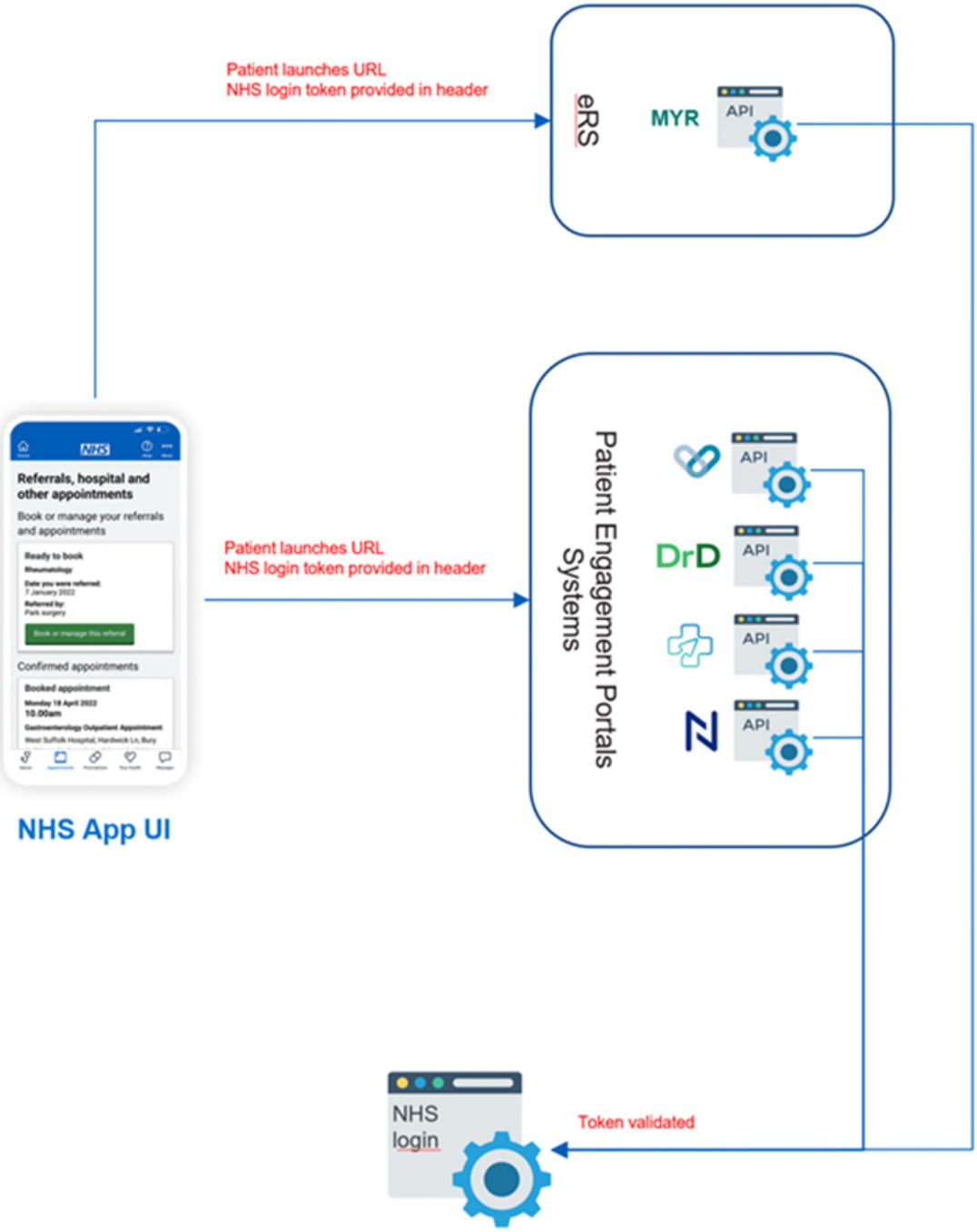
Authentication: Aggregator to eRS



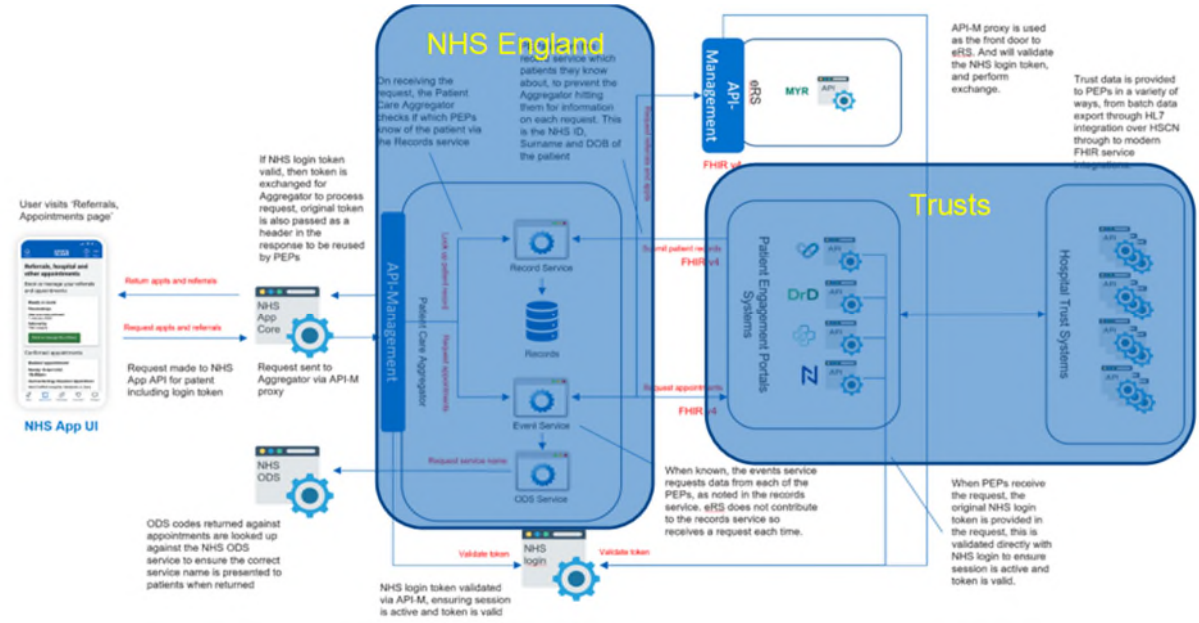
Steps 10 to 13

- The eRS proxy shall verify the same 'agg_apigee_access_token' access token for both eRS APIs.
- The 'agg_apigee_access_token' shall be used by the eRS proxy to retrieve the 'nhslogin_identity_token' and extract the patients NHS number.
- eRS will compare the NHS number from the 'nhslogin_identity_token' with the NHS number provided in the API request.

- This diagram is illustrative and shows a single authentication flow from the Aggregator which is the same for either eRS API being called.
- Data flows returning information from eRS back to users on the NHS App have been excluded.



NHS England is the data controller for the Aggregator in Phase 1. Trusts will continue to be data controllers of all data in their PAS systems and retain controllership of this data as it is processed by the Aggregator and the NHS App. Neither the Aggregator nor the NHS App creates new data - they merely aggregate and surface existing Trust controlled data.



Further enquiries regarding technical architecture, PEN testing and technical assurance can be made direct to the Wayfinder Programme at

england.wayfinder.pmo@nhs.net

Data Processing

Personal data:

NHS England are the data controllers in the first phase for the Care Aggregator, having both contract and Data Processing agreement with Servita (the data processor who built the Aggregator and who will manage live service support initially). NHS Digital will process personal data to the extent necessary to make available the relevant appointment information to the user through the NHS App, to meet the Purpose set out in the Direction. In the Beta first phase, NHS Digital do not collect or store patient data but surface the requested data from a deep link with the Patient Engagement Portal (PEP) of Trusts data.

The NHS App will present but will not store appointment information, which it will source from the Patient Care Aggregator.

The Wayfinder (NHS App) Services will not act as a patient record or the single source of truth for appointment information. This will remain with e-RS in the case of referrals and with the Trusts for outpatient appointments.

In addition, the Service will provide the ability to check if a patient is registered with the NHS App and provide access for the user to register if not already completed.

The data processed within the Aggregator Records Service is a minimised data set of:

- NHS Number

- Client ID for the Patient Engagement Portal (PEP) system where the NHS Number is located

No patient data is retained by either the NHS App or as a result of the processing journey with the exception of the Records area of the Aggregator where the NHS number persists. The Aggregator deletes the NHS number when there are no further forward appointments.

Non-personal Data (in isolation): (May also be considered as PID when used in combination with other identifiers)

Non-personal data used as part of processing:

- ODS Codes/ ODS Names
- Appointment Start Date/Time
- Referral Status
- Healthcare Service Appointment Type
- Specialty
- Appointment Type (could also be considered as PID in association with other data)
- Appointment Location
- Appointment Description

Further detail may be found in the DSMD (Data Standards and Mapping Document)

To deliver the Wayfinder (NHS App) Services, NHS Digital will conduct the following processing activities:

- The NHS Login token of the user is received by NHS App and validated with NHS Login via Application Programme Interface (API)-M
- On successful validation, the login token is retained and appended to a processing request sent to the Patient Care Aggregator via Application Programme Interface (API)-M. The login token can then be reused by e-RS and/ or the Patient Engagement Portal (PEP) system(s) relevant to the user's referral(s) and/ or appointment(s)
- The Patient Care Aggregator checks its Record Service for which Patient Engagement Portal (PEP) systems process data for the requested user
- Once the correct Patient Engagement Portal (PEP) systems have been identified, the Patient Care Aggregator's Events Service requests data directly from the relevant Patient Engagement Portal (PEP) systems. Simultaneously, the Events Service will request data from e-RS via Application Programme Interface (API)-M
- On receipt of the data request, e-RS and the Patient Engagement Portal (PEP) systems validate the Login token appended to the processing request directly with NHS Login
- Once validated, the Patient Engagement Portal (PEP) systems and e-RS return the requested data to the Patient Care Aggregator's Events Service.

Processing done outside NHS Digital

- Patient Engagement Portal (PEP) systems apply a series of business rules to exclude the following records from the feed to the Patient Care Aggregator:
  - users flagged by the Trust as not being allowed access via a Portal
  - users flagged with an 'S' code

- o Clinics that Trusts have indicated should not be visible to patients
- o Hidden appointments and appointments at ghost clinics
- o Appointments with specialties that Trusts have indicated should not be visible to patients
- The Patient Care Aggregator Events Service validates appointment information provided by e-RS and Patient Engagement Portal (PEP) systems with NHS Organisation Data Service to ensure the correct Service Name is presented to users.
- The Events Service applies a series of business rules to:
- o Restrict access to those under 16
- o Reject appointments from a Trust's secondary Patient Engagement Portal (PEP) where two are in use at a single Trust
- o Exclude appointments from specialist and mental health trusts
- o Exclude appointments in the past
- o Remove referrals that have already been booked
- o Map e-RS Referral State to NHS App Referral State, e-RS Appointment Type to NHS App Consultation Medium and e-RS Specialty to NHS App Specialty
- o Map Pending Portal Appointment Status to NHS App Appointment status (to cater for pending states)
- o Remove appointment date and time for referrals that use the e-RS Indirectly Bookable Service (to cater for instances where the agent booking the appointment on the user's behalf updates the hospital PAS system but not the e-RS record and they become out of sync)
- o Construct Appointment Description from PAS data, as attribute is used inconsistently across Trusts
- o Show the e-RS appointment information where information is present in both e-RS and Patient Engagement Portal (PEP) system
- Trust data is provided to Patient Engagement Portal (PEP)s in a variety of ways, including batch data export, HL7 integration over HSCN and FHIR service integration

The following tables provide:

- the detail on what personal/sensitive data is processed by the component parts of a user journey (yellow table)
- How a citizen can exercise their information access rights under UK GDPR (green table)

Personal Data Processed	NHS login	NHS App	Web NHS.UK	e-RS	Aggregator	NHS Trusts PEP incl service support*
Data Controller (DC) or Data Processor (DP)	NHSD, (DC)	NHSD (DC)	NHSD (DC)	NHSD (DC)	NHSE (DC), Servita (third party DP)	Each NHS Trust is DC for PAS data with PEPs as DP
Full name to correctly identify you.	✓	✓	✓	✓	✓	✓
Date of Birth to correctly identify you.	✓	✓	✓	✓	✓	✓
NHS number to correctly identify you.	✓	✓	✓	✓	✓	✓
Home Postcode or full address	✓			✓		✓
Telephone number	✓	✓	✓	✓		✓
Email address	✓	✓	✓	✓		✓
Third party contact details option if agreement provided to be contacted on behalf of other adults.		✓				✓
Photographic ID verification - login via NHS or Portal	✓					✓
Special Category (Health) Data Medical appointments		✓	✓	✓	✓	✓
Special Category data - Other clinical context, letters, tests, images, health information		✓	✓	✓	✓	✓
Automated decision making or profiling is not engaged in this service provision (Article 22 of UK GDPR)	X	X	X	x	x	x
Creation of unique reference codes				✓		✓

Information Access Right	NHS login	NHS Account	Web NHS.UK	e-RS	Appointments and Aggregator	NHS Trusts Portal Provider
Revoke consent	Consent is not the legal basis	Only where consent has been obtained i.e., participation in user research, surveys, and mailing list. App can also be deleted	Only where consent has been obtained	Consent is not the legal basis	Implied consent - user will need to contact NHS Trust - see PN or point of contact in-appointments section or via Portal provider.	✓Consent is not the legal basis for holding patient data. Where revoked for the NHS App, data will not be sent by NHS Trusts to Portal providers for the Appointments service and source data remains intact
To be informed (subject to ID verification)	✓	✓	✓	✓	✓	✓
To get access to it (Subject Access Request)	✓	✓	✓	✓	✓ may be redirected to hosts of source data	✓ Portals as processors will work with NHS Trusts. Patients may already be able to see their data digitally
To rectify or change it - errors	✓	✓	✓	✓	✓ may be redirected to hosts of source data	✓ Via NHS Trusts for the data they hold on PAS systems or by patient where user has provided information directly and digitally
To restrict or stop processing it	✓	✓	✓	✓	✓ may be redirected to hosts of source data	✓The data processor is instructed by the NHS Trusts as controller to stop sharing patient data with appointments service

Information Access Right	NHS login	NHS Account	Web NHS.UK	e-RS	Appointments and Aggregator	NHS Trusts Portal Provider
To transparency	PN https://access.login.nhs.uk/privacy#your-rights	PN https://www.nhs.uk/nhs-app/nhs-app-legal-and-cookies/nhs-app-privacy-policy/privacy-policy/	PN and all policies https://www.nhs.uk/our-policies/	PN https://digital.nhs.uk/services/e-referral-service/document-library/privacy-statement--nhs-e-referral-service	PN for NHS Account https://www.nhs.uk/nhs-app/nhs-app-legal-and-cookies/nhs-app-privacy-policy/privacy-policy/	PN provided by NHS Trusts as data controllers of patient systems via the Portal Provider. Alternatively, Portal Provider publishes an NHS Trusts approved PN.
To erase or remove it	✓ but not an absolute right	only for user research panel, survey, and mailing list data	only for user research panel, survey, and mailing list data	X	Limited and subject to redirection to host data	✓ But not an absolute right. Certain data may be erased but some source data will remain for provision of direct care.
To move, copy or transfer it	X	only for user research panel, survey, and mailing list data	only for user research panel, survey, and mailing list data	X	X	X
To object to it being processed or used	X	only for user research panel, survey, and mailing list data	✓ but not an absolute right	X	✓ but not an absolute right.	✓ but not an absolute right. Objection managed by NHS Trusts by instructing Portal providers
Information Access Right	**NHS login**	**NHS Account**	**Web NHS.UK**	**e-RS**	**Appointments and Aggregator**	**NHS Trusts Portal Provider**
To know if a decision was made by a computer without a person	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable
Cookie Policy information	https://access.login.nhs.uk/privacy#cookies	https://www.nhs.uk/nhs-app/nhs-app-legal-and-cookies/nhs-app-cookies-policy/	can be found within https://www.nhs.uk/our-policies/privacy-policy/	https://digital.nhs.uk/about-nhs-digital/privacy-and-cookies	NHS Account https://www.nhs.uk/nhs-app/nhs-app-legal-and-cookies/nhs-app-cookies-policy	Via each Portal providers information i.e., https://help.patientsknowbest.com/Cookies.html
Freedom of Information Request	✓	✓	✓	✓	✓	✓ NHS Trusts only as Portal providers are not subject to under FOI Act 3 (1)

*Can request to delete record from sponsor institution

In terms of **live services support,** where users encounter an issue with the Wayfinder (NHS App) Services, these will be managed as follows:

- Where the issue is related to the NHS App, NHS Digital will provide investigate per its standard operating procedure
- Where the issue is related to the aggregator, NHS England instructs NHS Digital to liaise with Servita on its behalf. Servita will investigate and respond to NHS Digital, who will respond to the patient on behalf of NHS England

NHS Trusts will manage their own information access and CRM responsibilities.

Legal framework and basis

DHSC has commissioned the service.

It is important to note that the initial launch of the secondary care appointments service via the Wayfinder Programme, described below, will be under short-term legal vires subject to change.

NHS England have the legal vires to collect the data from NHS Trusts into the Aggregator for the purposes of secondary care appointments in the NHS App through the following powers imposed by the NHS Act 2006:

- **The Duty of Enabling Patient Choice** - NHS England must act with a view to enabling patients to make choices with respect to aspects of health services provided to them. (NHS Act 2006, section 13I).

- **The Power to Obtain and Analyse Data** - NHS England can obtain and analyse data or other information for any purpose connected with the exercise of its functions in relation to the health service. (NHS Act 2006, Schedule 1, paragraph 13(3)

NHS England will provide Directions to NHS Digital. These Directions are given in exercise of the powers conferred by sections 254(1) and (6), section 260(2)(d), section 261(2)(e) and section 304(9), (10) and (12) of the Health and Social Care Act 2012 (the 2012 Act) and Regulation 32 of the National Institute for Health and Care Excellence (Constitution and Functions) and the Health and Social Care Information Centre (Functions) Regulations 2013 (the Regulations). These Directions are to be known as the “Wayfinder (NHS App) Services Directions 2022 “and come into force on the date signed. The purpose of these Directions is to enable NHS Digital to provide a service to NHS patients in England through the NHS App to securely view summary details of their scheduled appointments with acute NHS Trusts and to enable them to access further details about those appointments from the NHS App (the Purpose).

In accordance with Regulation 32 of the Regulations, NHS England directs NHS Digital to exercise such systems delivery functions of NHS England as are necessary for it to deliver the Wayfinder (NHS App) Services.

In accordance with sections 254(1) and 254(6) of the 2012 Act, NHS England directs NHS Digital to establish and operate such systems for the collection and analysis of information as are necessary to deliver the Wayfinder (NHS App) Services.

In accordance with section 254(3) of the 2012 Act, NHS England considers that the information which could be obtained by complying with these Directions is information which it is necessary or expedient for NHS England to have in relation to its exercise of functions in connection with the provision of health services.

NHS Digital is directed to provide the Wayfinder (NHS App) services unless and until new NHS App Directions are provided by the Secretary of State for Health and Social Care to replace the NHS Digital (Establishment of Information Systems for NHS Services: NHS App) Directions 20181 and which also direct NHS Digital to provide the Wayfinder (NHS App) Services (New NHS App Directions). These directions will be revoked from the date when the new NHS App Directions come into force.

In practice, this means that NHS England have invited Trusts to take part voluntarily under the basis as described above and in support of direct care purposes described in UK GDPR Art. 6(1)[e] and 9(2)[h]. The Records Service part of the Care Aggregator processes patient NHS numbers and allows the Events Service part of the Care Aggregator to retrieve patient appointment data. This is described in more detail in the bespoke section on the Care Aggregator.

NHS Trusts are able should they wish to enter into a DSA (Data Sharing Agreement) with NHS England to support the sharing of patient data - which does not in this instance create a joint controllership arrangement.

Should any Trust wish to receive a DSA template or send a completed DSA to NHS England, please use the email address as below:

england.ig-corporate@nhs.net

NHS Digital on the other hand are **not** collecting patient data but only providing the technological means via the NHS App, for patients to surface their own data. They cannot therefore issue in this first phase, a DPN (Data Provision Notice) to Trusts and indeed NHS England do not have the powers to do so either.

Further changes to these arrangements are anticipated later this year where

- NHS Digital will take over data controllership of the Care Aggregator and have their own contract and DPA with Servita
- There will be new Directions to NHS Digital for the NHS App's wider use including Wayfinder - from DHSC. These Directions will allow NHS Digital (now collecting the data) to issue a DPN to mandate the flow of data into the Aggregator for the purposes of the Wayfinder Programme.

The Aggregator is built by Servita as a data processor. As such, NHS England will be the data controller and put in place a valid contract and Data Processing Agreement. At some point in the future, this will move to the data controllership of NHS Digital. As the Aggregator is built in the NHS Digital environment, the Direction as described above, will detail its role and specification.

The NHS Trusts will remain as data controllers for their own PAS system data (for direct care). NHS England have the legal vires to collect the data from NHS Trusts into the Aggregator for the purposes of secondary care appointments in the NHS App through the following powers imposed by the NHS Act 2006:

- **The Duty of Enabling Patient Choice** - NHS England must act with a view to enabling patients to make choices with respect to aspects of health services provided to them. (NHS Act 2006, section 13I).
- **The Power to Obtain and Analyse Data -** NHS England can obtain and analyse data or other information for any purpose connected with the exercise of its functions in relation to the health service. (NHS Act 2006, Schedule 1, paragraph 13(3).
- **This can be supported by a Data Sharing Agreement (DSA) between each local NHS Trust and NHS England where the Trust requires this.** A template DSA can be provided for this purpose – NHS England is unwilling to enforce controllership or mandate the flow of data, and this will be down to each NHS Trust to decide and implement.

Portal providers as data processors: Existing contractual arrangements and Data Processing Agreements with their NHS Trusts will need to be reviewed to ensure they contain sufficient instruction to cater for the Wayfinder Programme requirements. Portal Providers are being onboarded by NHS Digital into NHS login and NHS App access via a SCAL assurance process (Supplier Conformance Assessment List) and subsequent Connection Agreement.

Data Protection Principles:
The UK GDPR, Article 5 (1) (c) states that personal Data shall be: “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;**”.**
A **minimum data set is processed** sufficient to unite the patient with their health information. This can be seen in a data processing table in the next section.
The UK GDPR, Article 5 (1) (b) states that personal Data shall be: “collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;”. The purpose is compatible with the original collection and processing, providing an NHS App route to complement the local service.

The use of Implied Consent refers to circumstances in which it would be reasonable to infer that the patient agrees to the use of the information, even though this has not been directly expressed. There are two elements to consider in the user journey:

- NHS login
- The agreement of each user to abide by the Terms of Use

The user is invited to share their **NHS login** credentials with the NHS App and again at the jump off point within the screen journey when they leave the NHS Digital environment and go to the Patient Engagement Portal (PEP) platform. These details were not given with an expectation of confidentiality where it is clear that these credentials are shared to gain secure access to the NHS App and any other connected services that are within the users

remit to decline or accept. This implied consent continues when the user is asked if they wish to remain in the confines of the NHS App or allow their NHS login credentials to be shared with an external party – the Patient Engagement Portal (PEP) – to view an enriched source of event/appointment data. A user can of course decline. However, acceptance is also part of the terms and conditions of use of the secondary care appointment service within the forward journey of NHS Trusts data.

By agreeing to those **Terms of Use**, the data subject then enters a contractual obligation with the service provider under UK GDPR Article 6 (1) (b) prior to 'jumping-off' into the forward service of the Patient Engagement Portal (PEP) on behalf of their data controllers, the NHS Trusts.

A privacy notice link (as well as Terms and Conditions) is provided in each screen footer to allow the user to make an informed decision before moving forward with the service. Progression assumes that the user has provided implied consent and then entered into an agreement with the provider.

The use of cookies - now that we have left the EU, the UK adheres to the Privacy and Electronics Communications Regulations (PECR, which describes the use of cookies) and not the EU's Privacy Directive for UK held data. Cookies policies need to be displayed alongside privacy notices to inform users about which type of cookies is present and why. The end-to-end user journey only engages with essential cookies for the purposes of surfacing secondary care appointments in the NHS App.

UK GDPR
For Servita and the Portal providers as data processors:
Article 6 (1)(b) processing is necessary for the performance of a contract and Article 9 (2)(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, or medical diagnosis, plus Part 1 Schedule 1 DPA18, para 2 health or social care purpose.

For NHS England, NHS Digital and NHS Trusts:
Article 6 (1)(e) processing is necessary for the performance of a task carried out in the public interest and Article 9 (2)(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, or medical diagnosis, plus Part 1 Schedule 1 DPA18, para 2 health or social care purpose.

Data controllership

The data processed to deliver the Wayfinder (NHS App) Services includes personal data and is subject to UK GDPR.

The first phase of Wayfinder will be under an interim measure as described in the legal basis section. This is further explained below in terms of data controllership.

Data controllership for PAS system data for direct care purposes, sits with NHS Trusts. Patient Engagement Portal (PEP) providers act as data processors. Portal providers and their respective sub-processors will all be acting as data processors to their respective NHS Trusts. They will be processing data under instruction from NHS Trusts and therefore applying the NHS Trusts legal basis to process data. NHS Digital will continue to seek technical assurance/competence from Portal providers through the established processes of SCAL completion (Supplier Performance Assessment Criteria**)** and Connection (of service) Agreements.

Through the NHS England direction to NHS Digital to collect/process data for the purpose of the Secondary Care Appointments Service in the NHS App, this will create the requirement for a joint data controllership arrangement between NHS England and NHS Digital for this purpose through a Provision of Service Agreement.

NHS England is the data controller in the first phase, for the Care Aggregator, built by Servita who act as the data processor for live service support.

NHS Digital, as the national information and technology partner for the NHS England health and care data systems will not be taking their more familiar role in the first phase of the programme. They will not be collecting or storing the patient data but facilitating its surface within the NHS App on patient request only.

The later changes: The temporary Direction from NHS England to NHS Digital will be replaced by a more enduring Direction from DHSC and this will allow a mandated collection of Trust data as a result of a Data Provision Notice (DPN) later this year. In addition, controllership of the Aggregator will at a later date move to NHS Digital. Further information on DPNs can be found at: https://digital.nhs.uk/about-nhs-digital/corporate-information-and-documents/directions-and-data-provision-notices/data-provision-notices-dpns

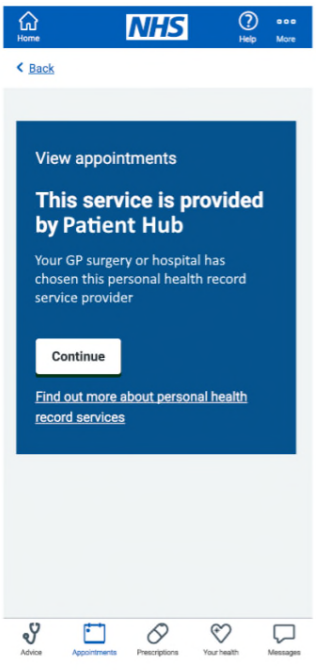
Privacy Notices (PNs):

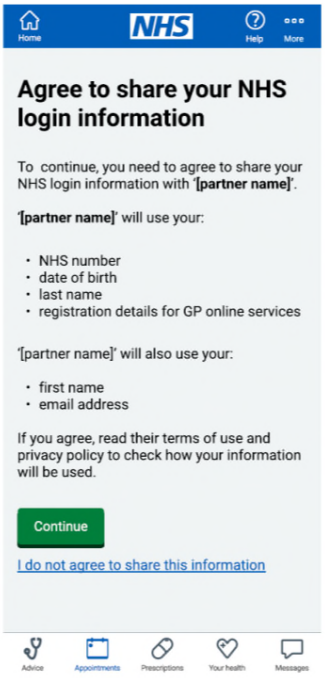
A privacy notice, terms of use, cookie policy and accessibility statement need to be available to patients through their user journey. The links to each notice have been provided as below:

Privacy Notice	Address
NHS login	https://access.login.nhs.uk/privacy
e-RS (with secondary care appointments)	https://digital.nhs.uk/services/e-referral-service/document-library/privacy-statement---nhs-e-referral-service
NHS App (with secondary care appointments)	https://www.nhs.uk/nhs-app/nhs-app-legal-and-cookies/nhs-app-privacy-policy/privacy-policy/
Patient Engagement	With a requirement to review/redraft their own PN to include that

Portal (PEP)s/NHS Trusts (As a multi tenanted or single tenanted arrangement),	non-App patients need to be aware of the use of their data by Patient Engagement Portal (PEP)s and the Aggregator

During the user journey, there will be a 'jump-off' screen where patients are invited to leave the area of the NHS App, share their NHS login details as credentials, and move to that of the Portal Providers and Trust. At this point, the user is not yet known to the Portal Providers but there remains a requirement to explain to patients what the processing will take place to allow them to decide whether or not to share their NHS login credentials. For certain types of Patient Engagement Portal (PEP)s, there will therefore be a footer link to a generic privacy notice containing sufficient detail regarding the processing to allow a user to decide as to whether they want to proceed to a Patient Engagement Portal (PEP). On the jump off screen PN, there will not be details of the Data Protection Officer. Other Patient Engagement Portal (PEP)s will have a different technical solution where the link leads to a search page which can look up a specific Trust. Once through this stage and onto the Portal Providers screens for their Trusts, a full PN will be available to allow a user to contact their data controller and exercise their privacy and information access rights. The screens below illustrate this point - the link will be in the footer on the left-hand slide.





The privacy notices within each portal domain will vary in presentation according to (1) the wishes/instructions of their respective data controllers and (2) whether the portal is a single or multi-tenanted entity. Single tenanted platforms will be able to provide a PN link in in-app screen footer to directly link each user with their bespoke NHS Trust. Multi tenanted platforms will be able to provide a link in their footer directing users to a more generic PN and further linkage as agreed by their data controllers. Full requirements for a PN once in the Portal area are as follows:

- Full contact details of the data controller and DPO (name, email, phone, address)
- the types of personal data collected
- where the controller obtains people's data if it wasn't from them
- why the controller has personal, sensitive, and confidential data and what they are doing with it (all types of processing)
- the lawful basis for processing
- who information is shared with (taken from the data flow in DPIA) and
- how long the controller holds people's information for before secure destruction
- Information access rights – which ones and how
- Cookie policy
- Terms of use

Use of the S-Flag and Excluded Patients Lists

(e.g., detainees, defence, vulnerable, mentally incapacitated and those requiring safeguarding).

Note: It is down to individual NHS Trusts to manage their clinical safety responsibilities.

S flags are a means of applying access restrictions to a patient's location data in their NHS record where there are known risks or vulnerabilities surrounding that individual. S-flags are unrelated to clinical priority. They are applied by the National Back Office (NBO) at the Patient Demographic Service (PDS).
As a result,

- Healthcare professionals in a Primary Care environment will be unable to access the patient's most up to date nationally held address/contact details and ODS code of GP practice - instead, they see an S-flag symbol.
- The patient will be unable to benefit from any national connected spine systems that require location information including:
    - Electronic Records Service (e-RS)
    - GP2GP
    - Summary Care Record (SCR) and
    - Elective Prescription Service (EPS)

In a Secondary Care Environment -

1. For NHS login and App - where a new NHS login is created at P9, account creation will be blocked where there is an S-flag. Where there is an existing user who already has an NHS login at P9, there is a check against a healthcare organisation's ODS code - which of course will be absent where an S-flag is present. This therefore limits a user's NHS functionality within the NHS App for e-RS and referrals and initial secondary care appointments cannot be surfaced.

2. For NHS Trust/Portal providers: The S-flag has been provided for primary care, up to the point of secondary care and not beyond. Portal providers are instructed by their NHS

Trusts (data controllers for PAS system data) to operate an 'Exclusion List' based on the local policy of each of their NHS Trusts. These policies vary from trust to trust meaning that exclusions can also be differently applied.

The clinical safety standards that include how to manage S-Flags, are mandatory in the NHS and those organisations not completing the obligations for Data Control Board standards - DCB 0160, would need to assess this as an organisation, operationally and clinically (patient safety). The standards offer a mechanism to assess digital clinical safety risks. If your organisation has not achieved DCB0160, you are encouraged to promote best practice by engaging with the requirements and manage the S flag risk through traditional risk logs in the interim.

NHS Trusts use of an Excluded Patient List:

NHS Trusts can create an **Exclusion List** of individual patients excluded from having data access via a Portal Providers and thus are excluded from registration notifications and receiving reminder notifications. This is necessary for those patients whose MYR/e-RS referrals/appointments were created BEFORE the patient was marked for sensitive processing, where data will still flow. Specific exclusions are honoured and decisions about them are taken at the Trust and portal level i.e., as near to the patient as possible and including the organisation with the duty to provide healthcare.

Note: NHS Trusts may make decisions to exclude certain cohorts from the MVP based on risk assessment i.e., Mental Health Trusts, specific clinics like sexual health, family planning and cancer, and self-declared opt-outs.

Exclusion	Description
NHS Trusts - specific	Currently there are two groups of Trust excluded for the MVP: Mental Health Trusts and self-declared opt outs
Specialty clinics if applicable	This is very specific to each Trust but may include perceived sensitive clinics like sexual health, family planning and cancer
''Dummy'' clinics	OP managers and administrators frequently need to change the management of clinics due to sickness, holiday, recruitment failures, etc or create new initiative clinics e.g., waiting list initiatives. To plan this, they set up dummy clinics which they can manipulate and confirm before sending patients formal confirmed appointment letters
Children under 16	Children at 16 and over can consent to health care but those under 16 are not. This is not completely true as some children have what is called Gillick competence (used in primary care assessment). As the mechanism of managing this through the App is not agreed as yet they have been excluded for now
Certain patients	There are two groups of people in this cohort; those with a

	sensitive (or “S”) flag on the personal Demographic System which is managed through their GP. It may include vulnerable people in witness protection, or in domestic abuse situations etc. The second group are identified by the Trust because of factors only known locally but could include issue related to mental capacity and clinical conditions

For further information on the S-flag can be found at the PDS National back Office:

https://digital.nhs.uk/services/national-back-office-for-the-personal-demographics-service/management-of-nhs-numbers-and-pds-records
and
https://digital.nhs.uk/services/demographics/restricting-access-to-a-patients-demographic-record

Age considerations for surfacing data within the NHS App

There is variation in how NHS Trusts apply age restrictions to the flow of data within their own Portal Providers systems. The Wayfinder Programme has confirmed requirements to be as follows:

Under 16s: Data will not flow into the Aggregator or records service or be surfaced within the NHS App for secondary care appointments. An additional error screen will be displayed to show to patients under 16 that the service is age restricted

16 and above: The NHS App Secondary Care Appointments service needs to provide information to those aged 16+ who have achieved P9 NHS login.

Some NHS Trusts will not be sending appointment data to the Aggregator until a patient is 18. **This is not in alignment with programme requirements** for a national product and is also not compliant with the BMA/GMC guidance and UK GDPR recognition that 16-year-olds are deemed competent to agree to share (and see) their medical data. However, if NHS Trusts have a **valid reason for excluding certain appointments** (as previously detailed in the Excluded List) for those aged 16+, the following screen message will appear to them:

If you are aged 16-17, you may not be able to view or manage some of your hospital appointments. This is because some NHS Trusts require you to be aged 18 or over to access these appointments.

If you are an NHS Trust that automatically excludes all patient data for those aged 16 and 17, you are advised to contact the programme for further guidance. It may be that you need to provide an explicit instruction in writing to your Portal Providers.

Once a young person reaches 16, data is inserted into the records service. The relevant portal informs the Aggregator, and the service is activated by the patient engaging with the

service. Whilst historic data will flow, it will not be displayed in the NHS App - only forward-facing appointments will show.

Glossary of Terms

Term or acronym	Meaning of term or acronym
Application Programme Interface (API)	Application Programming Interface
PEP PP	Patient Engagement Portal, a system provided by a 3rd party to NHS (Foundation) Trusts which provides online services (e.g., managing appointments) for patients of those (Foundation) Trusts Portal Provider
DPA DSA	Data Processing Agreement Data Sharing Agreement
e-RS MYR	e-Referral Service (service provided by NHS Digital) Manage Your Referral
DPIA	NHS Digital's requirement for data Security Protection Toolkit
MVP	Minimum Viable Product
SCAL (NHS Digital)	Supplier Conformance Assessment List
URL	Uniform Resource Locator
Deep link	Handoff to Patient Portal
ODS (code)	Organisation Data Search
PHR MRN	Patient Health Record Master Record Number
PMO	Project Management Office (Wayfinder) england.wayfinder.pmo@nhs.net

Project Sign Off

	Name	Job Title	Organisation	Date
Information Asset Owner	Morgan Thanigasalam	Clinical Lead Digital Clinical Safety Officer	Sherwood Forest Hospitals NHS Foundation Trust	14th September 2022
Data Protection Officer	Jacquie Widdowson	Information Governance Manager	Sherwood Forest Hospitals NHS Foundation Trust	13th September 2022
Information Governance	Gina Robinson	Information Security Officer	Sherwood Forest Hospitals NHS Foundation Trust	8th September 2022
Senior Information Risk Owner	Shirley Higginbotham	Director of Corporate Affairs	Sherwood Forest Hospitals NHS Foundation Trust	8th September 2022
Caldicott Guardian	David Selwyn	Medical Director	Sherwood Forest Hospitals NHS Foundation Trust	20th October 2022
Chief Digital Information Officer	Richard Walker	Chief Digital Information Officer	Sherwood Forest Hospitals NHS Foundation Trust	4th October 2022
Clinical Patient Safety	Morgan Thanigasalam	Clinical Lead Digital Clinical Safety Officer	Sherwood Forest Hospitals NHS Foundation Trust	14th September 2022

Assessment Summary

To be completed by Information Governance

Outcome of Data Protection Impact Assessment:	
1. Project/Implementation is recommended **NOT** to proceed, as significant corporate/customer risks have been identified.	☐
2. Project/Implementation to proceed once identified risks have been mitigated as agreed.	☐
3. Project/Implementation has met required legislative compliance and poses no significant risks. No further action required.	☒

Summary of Data Protection Impact Assessment; including legislative compliance and identified risks:
Summary: Legislative Compliance: Article 6(1)(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. Article 9(2)(h) allows processing for the provision of healthcare (direct care) or the management of healthcare systems (invoice validation, commissioner reporting, quality audits – essentially, mandated activity) Article 9(2)(i) allows processing for "ensuring high standards of quality and safety of health care." – which would cover research, audit, service improvement and addressing public health/inequalities **Summary of Risks**: Cyber security, loss of data, inappropriate access to data, inability to access data and Information Asset Management. **Risks** 1. Loss of system access/data - Full system back-up process in place. Annual penetration testing to be undertaken and the Trust to be informed of the outcome via the annual IAO process 2. Business continuity plans in each area, users have business continuity plans for their areas/departments. Not having these could lead to access to data or service delivery problems

3. Patients Know Best and Wayfinder will need to be added to the divisional information asset register and the data flows mapped and recorded as part of the annual IAO returns to the SIRO
4. Movers and leavers access not removed. Data is inappropriately processed and/or disclosed leavers' access not removed – PKB role 'Co-ordinator' manages professional access to PKB teams. (PKB Manual - Professionals (patientsknowbest.com)). Professional access at the Trust is currently very limited (not required for letters and appointments). As clinical teams go 'live' – a coordinator within that team will manage professional access. Individual username and passwords are provided. Each datapoint eg messaging in PKB has an audit trail.
5. non-App patients need to be aware of the use of their data by Patient Engagement Portal (PEP)s and the Aggregator

Recommendations for Action

Summary of Identified Recommendations:		
Recommendations: Information Asset Administrators to ensure Patients Know Best and Wayfinder are added to the information asset register and data flows are mapped and recorded Ensure business continuity plans are in place Account management Standard Operating Procedure to be generated and implemented, routine audit to take place Appoint coordinators within teams once clinical areas rollout	**Recommendation Owner:** IAA	**Agreed Deadline for action:**

Risk Template

For advice on completing this Risk Template please contact the Risk & Assurance Manager on x6326

Completed by:	Role:	Date completed:

Risk description What event could happen which would impact on the activity? What would cause it to happen? What would the consequence be?	**Primary controls** What is in place now to prevent the risk from occurring or to act as a contingency if it does occur?	**Current risk**			**Gaps in control** If the risk is not controlled to an acceptable level, what are the issues that need to be addressed?	**Acceptable risk**			**Mitigating actions required** What needs to be done to reduce the risk to an acceptable level?
		Consequence	**Likelihood**	**Rating (C x L)**		**Consequence**	**Likelihood**	**Rating (C x L)**	
Loss of system access/data due to connection failure or server failure either via NHIS or 3rd party supplier. This could result in the service being disrupted or unavailable. The consequences of this could be patient harm, financial penalties and reputational damage to the Trust	Full system back-up processes and ISO 27001 accreditation in place	2	2	4		2	2	4	Manual input, business continuity plan to be used

Risk description What event could happen which would impact on the activity? What would cause it to happen? What would the consequence be?	**Primary controls** What is in place now to prevent the risk from occurring or to act as a contingency if it does occur?	**Current risk**			**Gaps in control** If the risk is not controlled to an acceptable level, what are the issues that need to be addressed?	**Acceptable risk**			**Mitigating actions required** What needs to be done to reduce the risk to an acceptable level?
		Consequence	**Likelihood**	**Rating (C x L)**		**Consequence**	**Likelihood**	**Rating (C x L)**	
The system or service may not be able to operate due to system downtime or unavailability. Business continuity plans are not in place or available in each area.	Business Continuity plan for the Patients Know Best system is in place	3	1	3	Business continuity plan in place.	3	1	**3**	Business continuity plan reviewed annually.
If the system is not recorded on the information asset register, the system may not be brought back online in response to a cyber attack	In the Trust we have a business continuity plan if the service was unavailable. The department would default back to the current practice and access the records using the clinical systems at the Trust	2	2	4	Patients Know Best and Wayfinder will need to be added to the divisional information asset register and the data flows mapped and recorded as part of the annual IAO returns to the SIRO	2	1	**2**	Patients Know Best and Wayfinder will need to be added to the divisional information asset register and the data flows mapped and recorded as part of the annual IAO returns to the SIRO
Movers and leavers access not removed. Data is inappropriately	PKB role 'Co-ordinator' manages professional access to PKB teams. (PKB Manual - Professionals (patientsknowbest.com)). Professional access at the Trust is currently very	2	2	4		2	2	4	Appoint coordinators within teams once clinical areas rollout Routine audits.

Risk description What event could happen which would impact on the activity? What would cause it to happen? What would the consequence be?	**Primary controls** What is in place now to prevent the risk from occurring or to act as a contingency if it does occur?	**Current risk**			**Gaps in control** If the risk is not controlled to an acceptable level, what are the issues that need to be addressed?	**Acceptable risk**			**Mitigating actions required** What needs to be done to reduce the risk to an acceptable level?
		Consequence	**Likelihood**	**Rating (C x L)**		**Consequence**	**Likelihood**	**Rating (C x L)**	
processed and/or disclosed	limited (not required for letters and appointments). As clinical teams go 'live' – a coordinator within that team will manage professional access. Username and password controls in place. Account Management and access procedure to be completed. Each datapoint eg messaging in PKB has an audit trail.								

Risk Scoring Matrix.pdf

Legal Compliance

Compliance to be determined by IG team from the responses provided in the previous stages, delete as appropriate:

Data Protection Act 2018	Compliance and Comment
Principle 1 – Personal data shall be processed fairly and lawfully and, in a transparent manner	Lawfulness • We have identified an appropriate lawful basis (or bases) for our processing. • We are processing special category data and have identified a condition for processing this type of data. • We don't do anything generally unlawful with personal data. Fairness • We have considered how the processing may affect the individuals concerned and can justify any adverse impact. • We only handle people's data in ways they would reasonably expect, or we can explain why any unexpected processing is justified. • We do not deceive or mislead people when we collect their personal data. Transparency • We are open and honest, and comply with the transparency obligations of the right to be informed.
Principle 2 – Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes	• We have clearly identified our purpose or purposes for processing. • We have documented those purposes. • We include details of our purposes in our privacy information for individuals. • We regularly review our processing and, where necessary, update our documentation and our privacy information for individuals. • If we plan to use personal data for a new purpose other than a legal obligation or function set out in law, we check that this is compatible with our original purpose or we get specific consent for the new purpose.
Principle 3 – Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed	• We only collect personal data we actually need for our specified purposes. • We have sufficient personal data to properly fulfil those purposes.

Principle 4 – Personal data shall be Accurate and, where necessary, kept up to date, having regard to the purposes for which they are processed, are erased or rectified without delay	• We ensure the accuracy of any personal data we create. • We have appropriate processes in place to check the accuracy of the data we collect, and we record the source of that data. • We have a process in place to identify when we need to keep the data updated to properly fulfil our purpose, and we update it as necessary. • If we need to keep a record of a mistake, we clearly identify it as a mistake. • Our records clearly identify any matters of opinion, and where appropriate whose opinion it is and any relevant changes to the underlying facts. • We comply with the individual's right to rectification and carefully consider any challenges to the accuracy of the personal data. • As a matter of good practice, we keep a note of any challenges to the accuracy of the personal data
Principle 5 – Kept no longer than is necessary	• We know what personal data we hold and why we need it. • We carefully consider and can justify how long we keep personal data. • We have a policy with standard retention periods, however due to the Goddard Inquiry no destruction or deletion of patient records is to take place until further notice.
Principle 6 – Appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage	• We undertake an analysis of the risks presented by our processing, and use this to assess the appropriate level of security we need to put in place. • We have an information security policy (or equivalent) and take steps to make sure the policy is implemented. We have put in place technical controls such as those specified by established frameworks like Cyber Essentials. • We use encryption. • We understand the requirements of confidentiality, integrity and availability for the personal data we process. • We make sure that we can restore access to personal data in the event of any incidents, such as by establishing an appropriate backup process. • We conduct regular testing and reviews of our measures to ensure they remain

	effective, and act on the results of those tests where they highlight areas for improvement. • We implement measures that adhere to an approved code of conduct or certification mechanism. • We ensure that any data processor we use also implements appropriate technical and organisational measures.

Appendix 1 - Tabulated Legal Basis for End-to-end user Journey

Supporting Information for the Wayfinder Programme Joint DPIA

The legal basis across the user journey from NHS login to Patient Engagement Provider:

Note: UK GDPR (explicit) Consent (as per Art. 6(1)[a] and 9 (2)[a] - see end of document in full) will not be engaged in the end-to-end data process. Where the Common Law Duty of Confidentiality is engaged with Implied Consent for associated direct care purposes, the details are provided in the sections outlined below.

User journey point	Legal basis	Additional explanation
NHS login to NHS App	NHS Digital is the data controller for both login (SoS Direction to NHS Digital) and App (existing NHS England Direction to NHS Digital). Login is used purely to validate the request	NHS login provides identity assurance and enables a user to share their own credentials for access to services within the NHS App. This is **not** organisational data sharing or the sharing of confidential patient information and therefore the Common Law Duty of Confidentiality is not engaged.
NHS App to e-RS NHS App to e-RS **continued**	Part of the single sign on appointment interface. NHS Digital is the data controller for e-RS, under the Informatics Direction (amended) from DHSC. The existing Direction is deemed appropriate to engage with Wayfinder services where NHS England (as an appropriate body) has signed off the Servita SCAL (NHS Digital's assurance process - Supplier Conformance Assessment List).	This caters for the display of a patient's referral and first appointment in the provision of direct care, before a user's journey takes them forward to an enriched data source of appointments from the Patient Engagement Portal (PEP)s. No data from e-RS is stored in the Aggregator (Records service part) and this is a live feed display in the NHS App. The Information collected by e-RS is ● full name ● date of birth ● NHS number ● address ● telephone number ● email address (in the case of patients wishing to use an NHS login account to access Manage Your Referral) ● unique booking reference number

User journey point	Legal basis	Additional explanation
		• access code • service preference (which service(s) a patient is willing to have their referral sent to) • clinical context of a referral (this includes the specialty of a referral e.g., dermatology, cardiology etc.,) • referral letter detailing the specific clinical reasons for referral • blood tests • diagnostic test results (e.g., x-ray, MRI, ECG results etc.) • images • information from previous referrals, should this be relevant
NHS App to Patient Care Aggregator - with Aggregator Application Programme Interface (API) accessed through the NHS App. The Aggregator is being built by an assured third party (Servita), hosted within the AWS NHS Digital infrastructure under contract to NHS England NHS App to Patient Care Aggregator **continued**	NHS England will be the data controller for the service support and the Aggregator in the initial phases. NHS England and NHS Digital will be joint data controllers for the data surfaced in the NHS App where NHS England are issuing Wayfinder (NHS App) Services Directions (2022) to NHS Digital to provide the summary details of patient scheduled secondary care outpatient appointments in the NHS App. This will remain until the new NHS App Directions provided by the SoS for Health and Social Care replace the above mentioned. *This Direction is given in the exercise of powers under the Health and Social Care Act 2012 and Regulation 32 of the National Institute for Health and Care Excellence (Constitution and Functions) and the Health and Social Care Information Centre (Functions) Regulations 2013 (the **Regulations**).* NHS Digital is the data controller of the Application Programme Interface (API) Management System. NHS Digital are processing data	<u>Onboarding Patient Engagement Portal (PEP)s to Wayfinder</u> Where NHS Trusts - contract to a Patient Engagement Portal (PEP) and - has agreed to take part in 'Wayfinder,' The entire Patient Engagement Portal (PEP)'s list of NHS numbers is made available by a one-off bulk upload from that Patient Engagement Portal (PEP) to the Records Service (store) of the Patient Care Aggregator, except where the Trust, by instruction to the Patient Engagement Portal (PEP) has excluded certain data (e.g., specialist clinics) by maintaining their own Excluded Patient Lists. The data types collected and stored in the Records Service (ready to enable a live service interaction with the Events Service part of the Care Aggregator), are a patient's: NHS Number Patient Engagement Portal (PEP) unique ID

User journey point	Legal basis	Additional explanation
	under UK GDPR: - Art. 6(1)[c] - legal obligation by virtue of the Direction Art. 9(2)[g] - substantial public interest and Part 2 Sched.1, DPA 2018, para 6 (statutory and governmental process by Direction) Servita are a data processor of NHS England	The bulk uploaded data is subsequently updated periodically with data from the Patient Engagement Portal (PEP) to ensure the Records Service store is kept up to date. Users agree to share their NHS login credentials with the Care Aggregator and Patient Engagement Portal (PEP) (data processor) to be able to identify and see their full set of secondary care appointments, also known as events. This enables all patients to access their appointments via the NHS App, regardless of whether they have registered for a local Patient Engagement Portal (PEP) service (with separate local credential verification) or not. As stated previously, e-RS data is NOT stored within the Aggregator and is used for matching data in the live request, taking precedence over PAS appointment data where there is a conflict.
NHS Trusts to Patient Care Aggregator NHS Trusts to Care Aggregator, **continued**	In the host environment, this will be to provide health and care services under UK GDPR Article 6(1)(e) and for sensitive data Article 9(2)(h). NHS Trusts as data controllers, will not currently be mandated to provide secondary care appointment data to the Care Aggregator - their decision to send data will be voluntary. They will remain responsible for the management of an Excluded Patient List including those users that wish to remove their data from the Patient Care Aggregator Records Service.	NHS England have the legal vires to collect the data from NHS Trusts into the Aggregator for the purposes of secondary care appointments in the NHS App through the following powers imposed by the NHS Act 2006: ***The Duty of Enabling Patient Choice*** - NHS England must act with a view to enabling patients to make choices with respect to aspects of health services provided to them. (NHS Act 2006, section 13I). ***The Power to Obtain and Analyse***

User journey point	Legal basis	Additional explanation
NHS Trusts to Care Aggregator, **continued**	Note: - This is likely to change when the new NHS App Direction is in place between DHSC and NHS Digital and a DPN (Data Provision Notice) can be issued by NHS Digital to Trusts NHS England does not hold NHS Trust patient data and a patient's information access rights under UK GDPR will be executed by the NHS Trust as data controller for the care information they hold	***Data -*** NHS England can obtain and analyse data or other information for any purpose connected with the exercise of its functions in relation to the health service. (NHS Act 2006, Schedule 1, paragraph 13(3). <u>Onboarding NHS Trusts to Wayfinder</u> Where an NHS Trust - has agreed to take part in Wayfinder and - that Trust has been accepted by NHS England into the Wayfinder service Relevant GP Practice ODS codes for the Trust are enabled for Wayfinder services by NHS Digital via the existing NHS App system administration facility for controlling patient access to services available within the app. (All patients are associated with their GP Practice ODS code in the NHS App.) Where an NHS Trust is voluntarily sending the data to the NHS England Patient Care Aggregator, they are opting to do so to under powers identified by NHS England above: - This satisfies the condition of Common Law Duty of Confidentiality. - A minimum data set is processed (satisfying UK GDPR Art. 5(1)[c] - The purpose is compatible with the original purpose (UK GDPR Art. 5(1)[b], providing an NHS App route to complement the local NHS Trust - The data set is provided and shared for healthcare purposes, engaging implied consent. - The minimum data set is not

User journey point	Legal basis	Additional explanation
		considered to have been provided in confidence but for healthcare purposes. Implied consent is engaged in the flow of data from NHS Trusts to the Patient Care Aggregator. When a user clicks on the secondary care appointments link in the NHS App this causes the Care Aggregator to pull data from the Trust's Patient Engagement Portal (PEP) for a direct care purpose in order to display the Wayfinder screen within the NHS App. (The alternative of using explicit consent would require an additional screen and a method of recording a user's consent which is not practicable.) When a user then 'jumps-off' from the NHS App environment to the Patient Engagement Portal (PEP) provider's in-screen displays of enriched appointment data, they are doing so by informed choice (explanatory notes on screen, a Privacy Notice and Terms of Use - requiring acceptance) and agreeing to share their login details for this purpose.

- Article 6(1)(e): processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Article 9(2)(h): processing is necessary for the purposes of preventative or occupational medicine...medical diagnosis, the provision of health or social care or the management of health or social care systems and services…'