Document filename:	**NHS App - Data Protection Impact Assessment (DPIA)**		
Directorate / Programme	**NHS App**		
Document Reference	**NHS App/DPIA**	IAR0000718	
Information Asset Owner	[redacted]	Version	**3.00**
Author	[redacted]	Version issue date	**05/10/2026**

NHS App Data Protection Impact Assessment

Document Management

Revision History

Version	Date	Summary of Changes
0.1	08/05/2018	Initial Draft for Review
0.2	15/05/2018	Updated Section 3 Description of Processing & 5.8 Individual Rights / NHS Opt Out
0.3	12/06/2018	Updated Section 3 – Log Tracking & Vulnerable Groups, Section 4 Audience
0.4	08/07/2018	Updated response to Feedback and Guidance from [redacted]
0.5	23/08/2018	Updated to reflect new understanding of Data Controller and Processor roles in respect to different data sets
1.0	13/09/2018	Issued
1.1	18/09/2018	Updated after feedback from [redacted]
1.2	21/09/2018	Major changes due to DPO feedback
1.3	24/09/2018	Updated based on Legal feedback
1.4	12/12/2018	Review and update from [redacted]
1.5	19/12/2018	Update to include Akamai traffic routing
1.6	17/04/2019	Updated to include Organ Donation and rename Citizen ID to NHS login
1.7	29/05/2019	Update to include Nominated Pharmacy changes
1.8	31/05/2019	Update to remove NHS login geo locker statement and update the retention periods
1.9	20/06/2019	Port version 1.4 to DPIA v2.0 framework
1.10	18/07/2019	Updated and reviewed risks
1.11	30/09/2019	Updated to include risks associated with supplier ‘Controller’ assertion
1.12	06/11/2019	Updated to incorporate OLC.
1.13	01/10/2020	Updated in line with current features supported by NHS App to include the use of Qualtrics as the user research tool and Uplifted Legal Direction Specification
1.14	22/11/2020	Uplift to reflect Apps library updates
1.15	17/01/2021	Uplifted to reflect changes post NHS X issue of the draft legal direction
1.16	24/03/2021	Updated to reflect review comments from PTE.
1.17	26/03/2021	PTE Approval
1.18	08/10/2021	External Legal Review and Update
1.19	30/11/2021	Internal PTE and DPO Review and Update
1.20	28/03/2022	IAO and Programme Head Review
1.21	31/03/2022	PTE Review and update
1.22	22/06/2022	Updated to include more detail on NHS App Messaging and Push Notification service pilot and minimum viable product (MVP)
1.23	20/10/2022	Amendments following reviews
1.24	31/01/2023	Update to reflect NHSD and NHSE merger

1.25	18/09/2023	Updated to include integration with EPS Prescriptions for Patients API
1.26	21/05/2024	Updated to reflect • Presentation and contact information amendments • General updates / inclusion of NHS Wayfinder (sections 11, 12 and 15) • Test results data extract (analytics) to inform prioritisation and service design decisions for feature iteration and improvements (section 5.8).
1.27	22/07/2024	Updated to –reflect • MVP process with accessing past and future appointments through NHS Wayfinder • MVP retention application • Outline anonymous statistics around NHS App loading for users
1.28	01/04/25	Updated to reflect • Consolidation of information in sections 14-15 • Addition of information relating to NHS App analytics data migration to NHS FDP • Interim review of data security and compliance risks s16
1.29-1.43	23/07/25	Between versions 1.29 and 1.43, this document underwent an iterative internal update process to reflect feedback from key stakeholders and alignment with evolving operational requirements. The cumulative updates include: • Sections 1-15 – Consolidation of information • Section 16 – Full review of data security & compliance risks in section 16 • Addition of Annexes • Document reformatting and general editorial improvements
1.44	17/10/25	Updated reflecting feedback from 2nd line review
1.45	23/02/26	Updated reflecting feedback from DCG/review: • Section 7 - Minor clarity edits on process for how users can access their rights to their data • Section 16 - Clarity on scope of risks, new risks (17-21) and progressed risk information updates
2.00	22/06/26	Issued
2.01	11/06/26	Updated • Section 8 - Clarification to the justification of the processing of NHS Numbers in Proxy use cases • Section 16 – New risks (23, 24), progressed risk information and risk scoring re-alignment with updated NHS England Risk Management Framework • Section 19 – Summary of high residual risks (based on the above amendment)
2.02	31/07/26	Updated: • Section 11 - Cross-references to NHS App Analytics DPIA and NDC DPIA re: retention of analytical data supplied to FDP • Section 11 – Minor clarifications to database names to align with NHS App Information Asset Register
2.03	10/08/26	Updated Section 4 to include Internal-only temporary analytical data extracts performed by NHS England Health Information services.
2.04	10/09/26	Updated: • Sections 2 and 4 – Revised to include NHS App front-end interaction data captured and retained in Adobe Analytics separate to back-end operational analytics dataset captured and retained in the NHS App Analytics Store, NDIT and the Federated Data Platform. • Annex A – New reference for the NHS App ‘add to native calendar’ feature
3.00	22/09/26	Live version

Reviewers[1]

This document must be reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version
[redacted]	Cyber Security	23/01/2026	1.43
[redacted]	Deputy Director IG Delivery (Digital & Operations) – **2nd Line Review**	15/08/2025	1.43
[redacted]	Deputy Caldicott Guardian	17/10/2025	1.44
[redacted]	Data Protection Officer	17/10/2025	1.44
[redacted]	IG Lead	23/06/2026	3.00

Approved by

This document must be approved by the following people:

Name	Title / Responsibility	Date	Version
[redacted]	Director of Privacy and Information Governance	22/06/26	1.45
[redacted]	NHS App IAO	17/08/2026	2.03
[redacted]	NHS App IAA	10/09/2026	3.00

Document Control

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

[1] This table reflects the most recent version reviewed by an individual.

Table of Contents

Document Management 2
Glossary of Terms 6
Purpose of this document 7
Introduction 8
1. Consultation with Stakeholders 9
2. Data Flow Diagram(s) 11
3. Purpose of the data processing and data controllership 16
4. Description of the Processing 18
5. Describe the legal basis for the processing (collection, analysis or disclosure) of personal data 25
6. Demonstrate the fairness of the processing 28
7. Ensuring individuals are informed about the ways in which their personal data is being used 29
8. Is it necessary to collect and process all data items? 31
9. Describe if personal datasets are to be matched, combined or linked with other datasets (internally or for external customers) 35
10. Describe if the personal data is to be shared with other organisations and the arrangements you have in place 36
11. Describe how long personal data is retained 38
12. Where you are collecting personal data from the individual, describe how you will ensure it is accurate and if necessary, kept up to date 40
13. How are individuals made aware of their rights and what processes do you have in place to manage such requests? 41
14. What technical and organisational controls for “information security” have been put in place? 42
15. Where personal data is stored or processed 44
16. Identification of Risks and Measures to control/mitigate (treat) 45
19. Further Actions 88
20. Signatories 88
21. Summary of high residual risks 89
Annex A – NHS App features – further details 91
Annex B – NHS App Notification and Messaging Services - Controller Table 94
Annex C – NHS App third-party products and integrations 97
Annex D – Subsidiary Risks transitioned to NHS App programme team registers: 104
Annex E - 2 Year past appointment retention – Now Closed 114
Annex F – Glossary of terms (full descriptions) 116

Glossary of Terms

For full descriptions of these terms and definitions please refer to Annex I

Term	Definition
API	Application Programming Interface
BAU	Business As Usual
CCS	Crown Commercial Service
CSP	Cloud Service Provider
DARS	Data Access Request Service
DHSC	Department of Health and Social Care
DOS	Digital Outcomes and Specialists (procurement framework)
DPIA	Data Protection Impact Assessment
DSPT	Data Security and Protection Toolkit
EPS	Electronic Prescription Service
FDP	Federated Data Platform
FHIR	Fast Healthcare Interoperability Resources
GPIT	General Practice IT
ICB	Integrated Care Board
IM1	Interface Mechanism 1 - standard NHS GP system interface
NDC	National Digital Channels
NDIT	National Data Ingestion Tenant
NDOO	National Data Opt-Out
NHSA	National Health Service Act (Isle of Man)
NICE	National Institute for Health and Care Excellence
OLC	Online Consultation
ODS	Organisation Data Service
PET	Privacy Enhancing Technology
PHR	Personal Health Record
PID	Personally Identifiable Data
RDDT	Regional Director of Digital Transformation
SLSP	System Level Security Policy
SME	Subject Matter Expert
SMS	Short Message Service (text messaging)
Spine	The central NHS infrastructure that connects different systems
UK GDPR	United Kingdom General Data Protection Regulation
WAF	Web Application Firewall
Wayfinder	NHS system for aggregating and presenting referral data from secondary care
e-RS	e-Referral Service

Purpose of this document

A Data Protection Impact Assessment (DPIA) is a useful tool to help NHS England demonstrate how we comply with data protection law. This document can be made available upon request to the public. DPIAs are also a legal requirement where the processing of personal data is “likely to result in a high risk to the rights and freedoms of individuals”.

This DPIA has been conducted for the NHS App and has been refreshed pursuant to the issuing by the Secretary of State of the NHS App Directions 2023.

Introduction

Vision

To be the digital front door to the NHS[2]. This will be achieved when a third of patient interactions with the NHS are delivered through digital channels.

Objectives

1. **Improve health outcomes** and support users to prevent, improve and manage ill health by:
    - putting them in control of their own health and care, and the health and care of those they care for
    - supporting users to navigate the health system and be directed to the right care setting
    - increasing their skills, confidence, knowledge and capacity for self-advocacy
    - giving the public access to high quality, efficient and safe digital services with the aim of achieving better health outcomes for individuals and populations
2. **Drive efficiencies and reduce burden**, restoring capacity to the frontline and reducing administrative overheads by:
    - increasing users' ability to self-serve, e.g. booking and managing appointments
    - supporting operational efficiency, e.g. reducing do-not-attends
    - reducing operational costs, e.g. replacing SMS with NHS App messages
    - helping users get to the right place, first time
    - designing NHS App services in a way that supports health system KPIs
    - delivering a service with consistent quality, safety, and security and which meets the range of user needs

NHS App Key Performance Indicators

- Monthly journey completions
- Level of clinical risk
- Quality of end-to-end experience
- NHS productivity savings
- NHS App operational costs

Delivery methods to achieve objectives include:

- improving access to and uptake of core digital health journeys
- validating emerging use cases and enabling technologies
- investing in capabilities to make the NHS App sustainable.

[2] As one of the NHS National Digital Channels (NDC)

1. Consultation with Stakeholders

Stakeholder engagement has been built into the process for conducting the DPIA and associated review and refresh[3]. Key stakeholder types are outlined below:

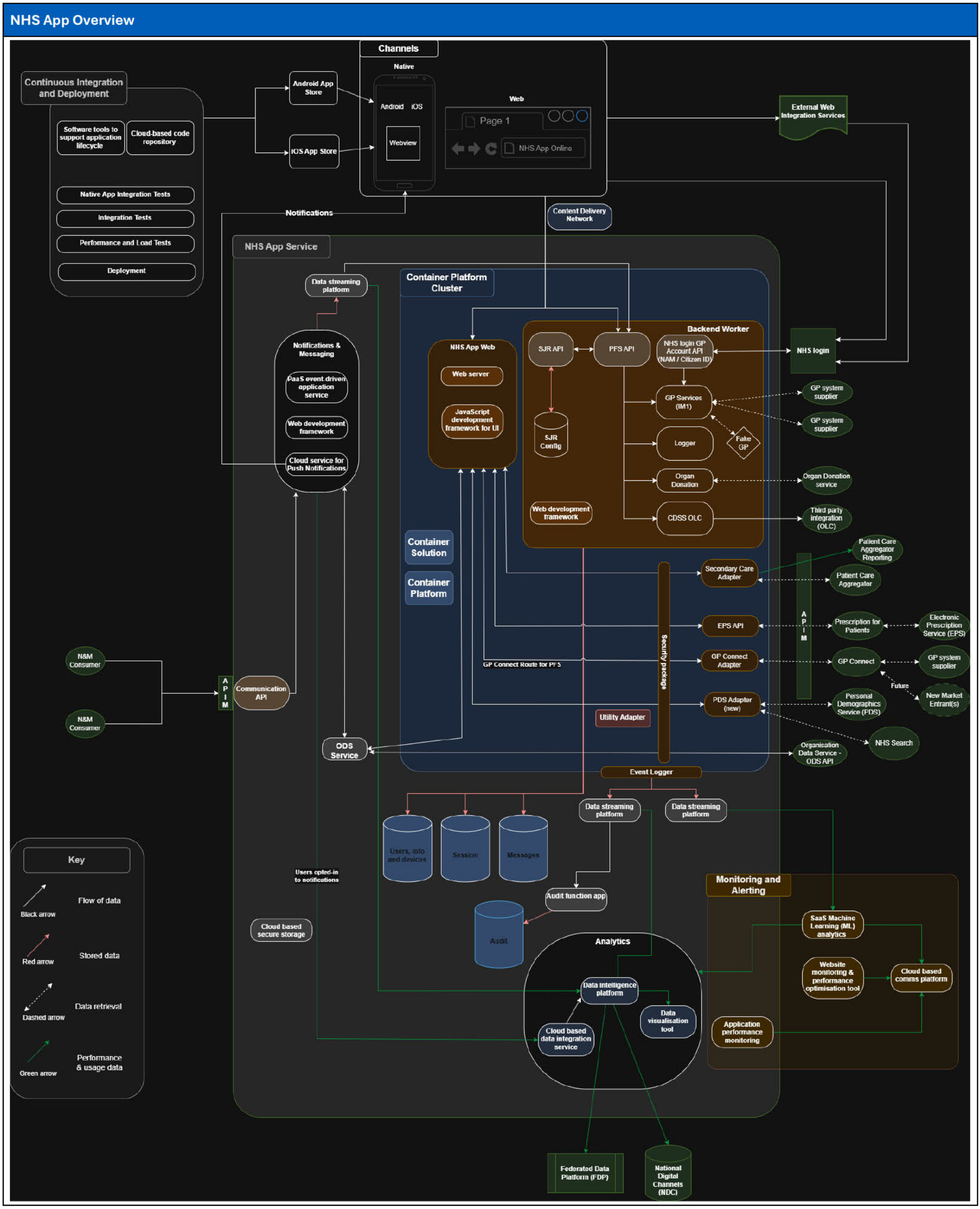
Stakeholder type	Detail of engagement
Users	At any time, users can provide feedback via the App itself on their experience using it. In addition, users are regularly engaged on new changes to content for user-facing parts of the NHS App conducted through: Surveys, interviews, focus groups and online studies. Whilst the focus of this engagement is more on the features, user comprehension of data processing is included proportionately when it applies. (e.g. User testing for a design uplift of the Organ Donation decision [Feb 2025] involved testing whether users were clear about the decision they had made, where this information was held, how it was being used etc).
Commissioners	Engagement for presenting NHS App feature updates, comms campaigns and data and gathering of feedback will cover data sharing proportionately. This is done through the following BAU mechanisms: • Monthly Regional meetings • ICB digital boards • ICB community of interest group • Quarterly strategic forum with RDDTs[4] • Regional NHS App training In addition, the team handles enquiries and feedback from the system on an ongoing basis.
Clinicians	Engagement with clinical stakeholders at the onboarding of any new or upgraded NHS App features consider strategic clinical issues and consult with clinical SME with domain knowledge ahead of national implementation. In addition, clinicians and staff in services are consulted as part of user research. Data sharing is covered proportionately through these processes.
Department of Health and Social Care (DHSC)	DHSC are engaged as part of the process any updates to or approvals of Directions or specification. The Joint Transformation Unit reviews and approves any updates
Internal and External legal advisors	Occurred at inception. Engagement is also sought on an as needs basis where risks or issues have been identified.

[3] Consultation on further changes will occur where required and this section will be updated when consultation is done.
[4] Regional Directors of Digital Transformation

Stakeholder type	Detail of engagement
	Would also be considered if any major or complex changes are required to the Directions.
Internal Stakeholders	Proportionate and ongoing interface with key internal stakeholders through NHS England's governance and account management for: • Legal and Information Governance • Commercial • Cyber Security • Clinical Safety
GPIT Communications suppliers	Occurred at inception and continues on an ongoing basis as per the processes and standards in place for introducing new changes relating to GPIT systems.
Ofcom	Occurred at inception.
Digital First Primary Care	Occurred at inception.

2. Data Flow Diagram(s)

The diagram below provides a high-level overview of the data flows from and to the NHS App.



NHS App Messaging and Push Notifications Service

The NHS App messaging service provides a secure inbox that allows patients to receive messages from health and care services such as their GP surgery via the NHS App, instead of SMS (text message) or letter.

Patients will get a notification from the NHS App when they receive a message in their secure inbox, if they have notifications enabled on their device.

There are three features offered as part of the NHS App Messaging and Push Notifications Service:

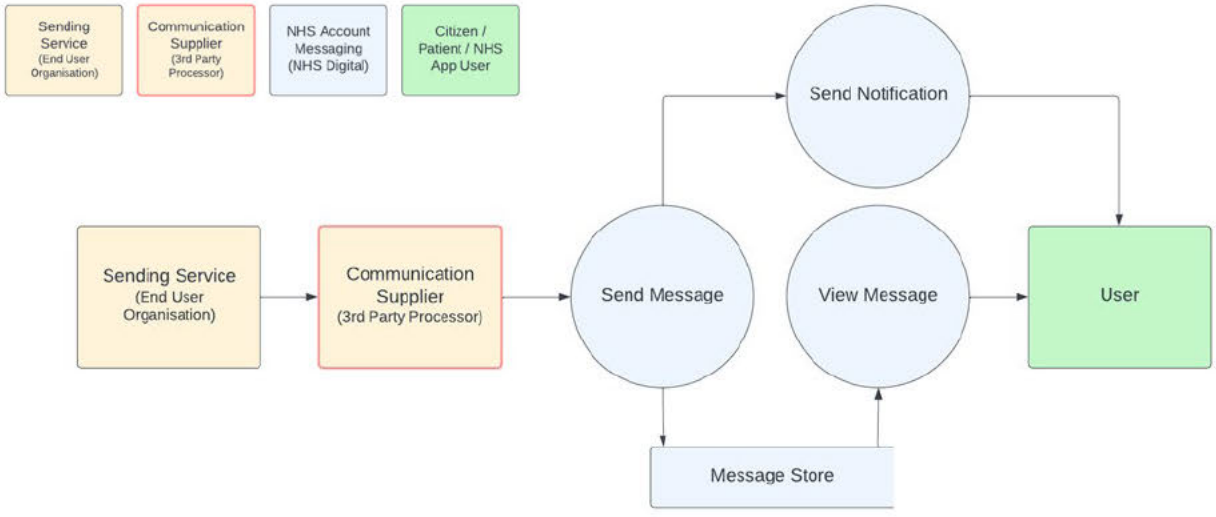
1. Send & View Messages
2. Check User Details
3. Check Message Status

There are up to four actors/entities involved in the end-to-end service:

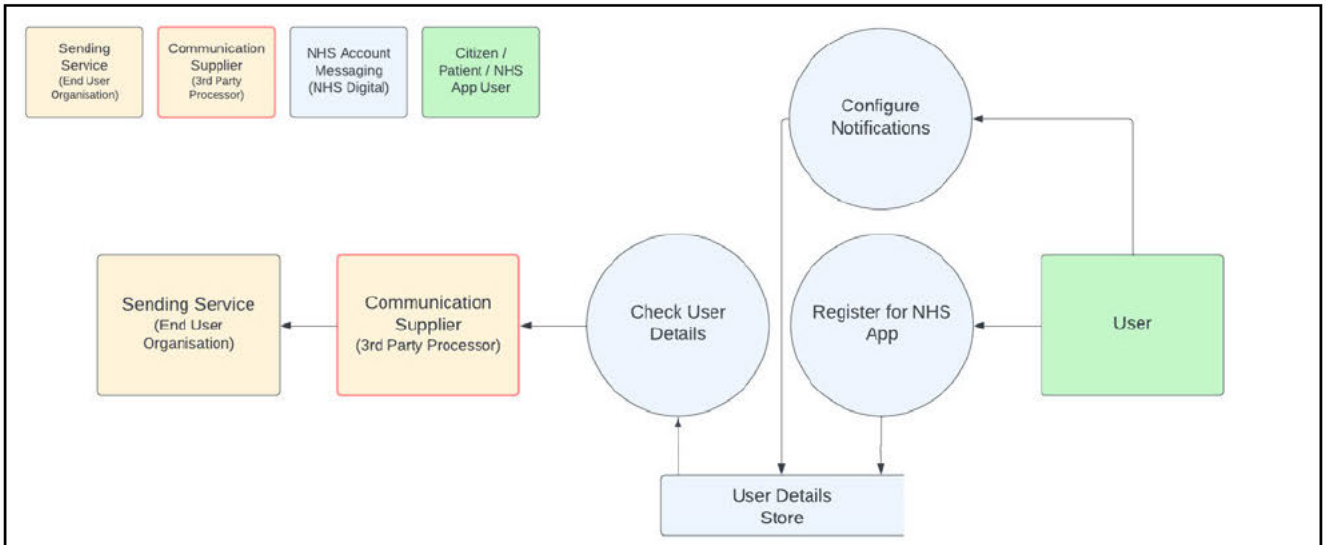
1. **Required:** Sending Service
2. **Optional:** Communication Supplier; as a data processor appointed by the Sending Service
3. **Required:** NHS App Messaging and Push Notifications Service (part of NHS England)
4. **Required:** Citizen / Patient / NHS App User

Please see diagrams 2.1-2.3 below for data flow with respect to this service

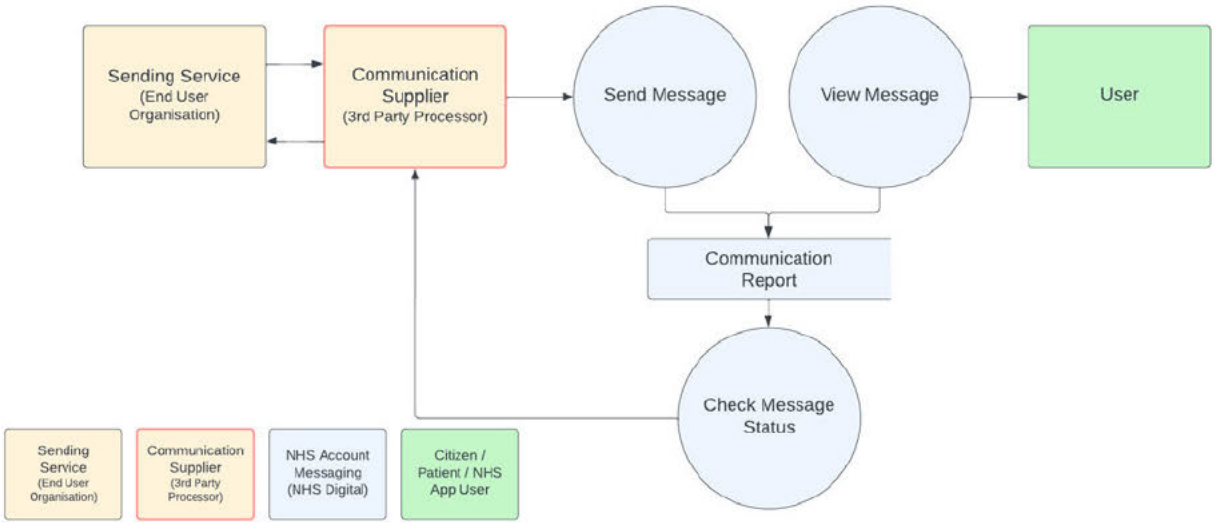
2.1. Send and view messages



2.2. Check New User Details



2.3. Check Message Status



NHS App operational Analytics – Databricks and the Federated Data Platform

The NHS App Analytics dashboard gathers metadata of events in the metrics/analytics data on the usage of the NHS App[5]. This data reflects how end users interact with the NHS App – for example login activity, prescription ordering, health record views. The information is used to identify improvements to the service and publish statistics to the wider NHS as to the savings and efficiencies provided by the NHS App.

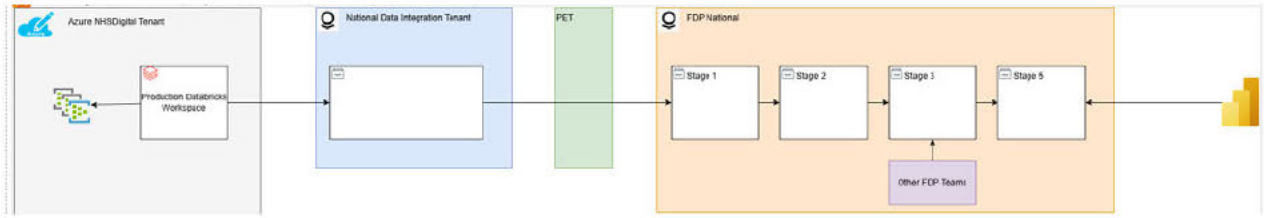
To help local trusts, Integrated Care Boards (on behalf of the integrated care systems) and NHS England proactively plan services that meet the needs of their population. This information will transition to the NHS Federated Data Platform (FDP).[6]

The following diagrams represent the transition of the NHS App Analytics dashboard from Azure Databricks across to the NHS FDP data platform (hosted in AWS). Currently the

[5] Whilst event data will be linked to an NHS Number, only metadata is collected, no sensitive details. See section 4 for more information on analytics data

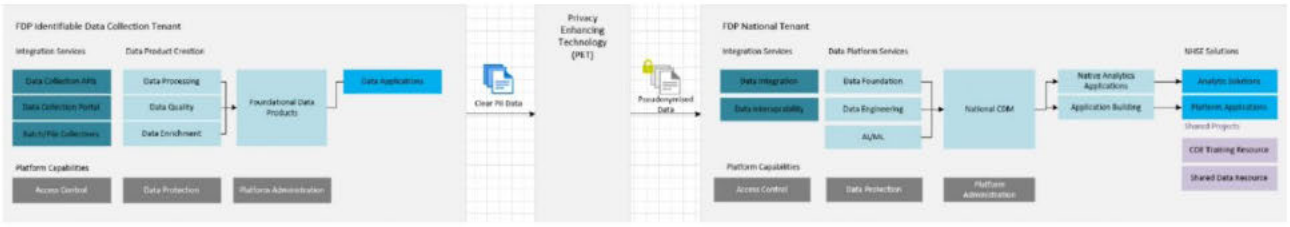
[6] Transitioning 2025. NHS FDP: https://www.england.nhs.uk/digitaltechnology/nhs-federated-data-platform/. Further information is available in the DPIA for NHS FDP.

Analytics data is hosted in Databricks will be migrated across, and Databricks will be retained as part of the secure transport layer of the data across to the Federated Date Platform (FDP).



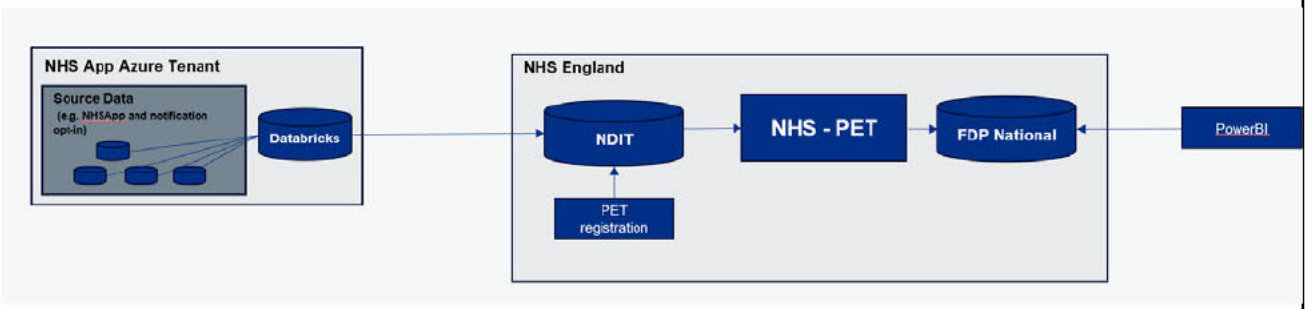
Once the metrics/analytics data4 is received by the NDIT platform, it enters the Federated Data Platform (FDP) where it goes through the following steps:

- The following PID items are first stored in the identifiable data area: NHS Numbers, NHS Login IDs and ODS codes
- These PID items are then processed using NHS Privacy Enhancing Technology (PET) (pseudonymisation)
- After this, is the data is aggregated with the non-personal data in the FDP National Tenant.



Once the data lands in the Federated Data Platform, it will transition through a tiered data cleansing and refinement process to enhance accuracy, quality and usability (Medallion architecture Bronze, Silver and Gold) - with the final gold layer having non-identifiable aggregated data. All PID data will go through a Privacy Enhancing Technological process to Pseudonymise the fields into non-PID data. The PID fields that will go through this Pseudonymisation process are:

- NHS Number
- NHS Login Id
- ODS Code



NHS App interaction analytics – Adobe Analytics

Where a user has enabled optional analytics, defined interaction events and associated technical and contextual data are captured directly from the NHS App and sent to Adobe

Analytics. This supports analysis of how users interact with individual features and journeys, including journey progression, completion, drop-off points and service performance.

Adobe Analytics is a separate destination and dataset from the NHS App operational analytics data processed through Azure Databricks, the National Data Ingestion Tenant and the Federated Data Platform. Data captured in Adobe Analytics is not automatically transferred into the Databricks/FDP analytical flow.

Further information about the Adobe processing arrangements is provided in the National Digital Channels Adobe Analytics Cross Channel Tracking DPIA.

3. Purpose of the data processing and data controllership

The Data processed by the NHS App services will be used for:

- Giving the public access to high quality, efficient and safe digital services with the aim of achieving better health outcomes for individuals and populations.
- Delivering a service with consistent quality, safety, and security and which meets the range of user needs.
- Providing secure access to systems by integrating with the Identity Verification and Authentication solution provided by NHS login.
- Supporting commissioners and policy teams by providing anonymous statistical data which may be used to understand health issues and challenges better; and (where reasonably required) enable the NHS App Services to be delivered.[7]
- Supporting strategies which may improve health outcomes for the population and reduce inequalities in health.

Further information on App features is set out in Annex A

Data Controllership

Purpose	NHS England	Secretary of State	GP Practices	Healthcare Providers
Processing personal data made available to the NHS App by GP system suppliers*	No	No	Yes	No
Facilitation of transmission between NHS and GP system suppliers*	Yes	Yes	No	No
Collecting and analysing data	Yes	Yes	No	No
NHS App Messaging and Notifications: content via NHS Notify (depending on sending service)	Yes[8]	No	Yes[7]	Yes[7]
NHS App Messaging and Notifications: facilitation of transmission and storage	Yes	Yes	No	No
All other aspects of the NHS App	Yes	Yes	No	No

*The NHS App Service processes personal data, which is made available to NHS App users, GP system suppliers by GP practices. GP practices are Data Controllers for this data. To the

[7] See Annex G for an example through a temporary Health Information analytical extract

[8] Only if sending the message

extent that NHS England facilitates the transmission of this data, it acts as a Data Controller independent of the GP Practices (as part of its Joint Controller arrangements with the Secretary of State arising from the NHS App Direction 2023 and associated Requirements Specification). This is to enable the services requiring transmission of personal data from GP Practices on the NHS App to be delivered.

NHS England and the Secretary of State as Joint Controllers determine the purpose and means by which such transmission of personal data takes place in the NHS App, but in all other respects the GP Practice is the Data Controller of such personal data. This role of NHS England as a joint controller with the Secretary of State applies where files containing personal data are surfaced in the NHS App – for example, during a file upload or download and notification or messaging action as part of the provision of online consultation (OLC) and patient health record (PHR) services.

4. Description of the Processing

Nature of processing

How data is collected
Primary Care
The NHS App integrates with the GP system suppliers to allow App users to use features that retrieve data from primary care (e.g. view their medical records). This is facilitated through the following Application Programming Interfaces (APIs): • The Interface Mechanisms (IM1) for practices supplied by EMIS (EMIS Web product), TPP (SystmOne product) which accounts for over 99% of GP practices in England. • A set of standardised Fast Healthcare Interoperability Resource[9] (FIHR) APIs from GP Connect for practices that are supplied by Medicus.[10]
Secondary Care
Secondary care (past and future) appointment and referral data is pulled from the Patient Aggregator (NHS Wayfinder) with Waiting Time data pulled from the My Planned Care dataset. **Wayfinder:** The NHS App integrates with Wayfinder, to enable App users to view their secondary care referrals and bookings. NHS Wayfinder consolidates data from secondary care providers and the national e-Referral Service (e-RS). The NHS app requests a summary of their referrals and bookings from Wayfinder. **My Planned Care:** The NHS App integrates with this dataset, which compiles waiting list data. This allows App users to view relevant average waiting times based on their specific speciality and trust.
NHS Login
Data is collected from NHS login during the identity verification and authentication process to ensure secure access to NHS App services. When a user registers or logs into the NHS App, NHS login collects and processes the personal information required to verify identity (e.g. the user's name, date of birth, contact details etc). This data is securely processed to confirm the user's identity and provide authenticated access to the NHS App. Once verified, the NHS App uses this authenticated session to securely retrieve and display relevant health information from GP system suppliers.
Notifications and Messaging
The content of In-app messages and notifications is stored in the NHS App to support users with communication and actions related to their healthcare.

[9] FHIR is a quality standard for exchanging healthcare information electronically
[10] Access may be limited depending on the GP practice sign-up to GP Connect

Messaging: When healthcare providers send messages via the NHS App, the content is securely stored within the App itself. These messages may include personal data, and, in some cases, special category data related to the user's health (see section 8).

- As per section 3, it is the GP practice/sending healthcare provider who is the data controller for in-app message content. NHS England is the data controller in terms of facilitating the communication and displaying messages in the NHS App.
- Healthcare providers are advised to limit the inclusion of extensive healthcare information in messages. This practice reduces the amount of sensitive data stored within the app, aligning with data minimization principles.

Notifications: When the NHS App sends alerts to a user's device to inform them about updates or actions related to their healthcare (e.g. upcoming appointments, new messages from providers etc) it collects only the essential data required to deliver notifications effectively – the unique identifier for the device, and the user's choices regarding which types of notification they wish to receive and how they wish to receive them (notification preferences).

Log and analytics

Databricks/FDP

NHS App operational analytics data is processed through Azure Databricks/NDIT and FDP to support aggregated dashboards, operational reporting, service planning and publication of statistics via the National Digital Channels programme and the Federated Data Platform. The data items, data flow, access arrangements and retention applying to this dataset are described separately below.

Adobe Analytics

Where a user has consented to optional analytics, defined interaction events and associated technical data are sent from the NHS App to Adobe Analytics to understand use of individual features, user journeys, drop-off points and service performance. This processing is distinct from the operational analytics dataset processed through Databricks and FDP.

Please refer to the National Digital Channels Adobe Analytics Cross Channel Tracking DPIA for further information

Internal-only temporary analytics extracts

Temporary analytical extracts may be created from existing NHS App GP record data to support the design and improvement of NHS App Health Information features. These extracts are held internally within the NHS England programme team and used to understand the structure and completeness of record data and do not contain direct patient identifiers or free-text content.

How data is used

The NHS App primarily functions as a platform that allows users to access and view their personal health information without storing this data on the device itself.

For example, when users use the App to access their GP health record, the data is retrieved in real-time from the GP surgery's systems of the user. It is then displayed on their device.

This means the app does not permanently store the user's GP records; it simply provides a secure interface for viewing them.

Having said this, the NHS App does collects and processes the following types of operational data tabulated immediately below, which will include personal data items[11] (see section 8 for further details)

- **Audit data:** Helps maintain security and resolve technical issues
- **Messaging data:** Facilitates communication between users and their healthcare providers
- **Performance data:** Monitors performance and improve services
- **Session data:** Maintains login status and ensure secure interactions

NHS App users (including NHS staff) may submit support queries via supplier-managed service desk channels (e.g. webforms or B2B portals). In some cases, patient-identifiable data (PID) may be included in the submission to support technical triage. This data is processed solely by the supplier for the purpose of NHS App support, is not accessed by NHS App teams, and is subject to access control, retention limits, and information governance prompts. The NHS App team defines the purpose of support handling but does not process or store the data directly.

How data is stored

All data stored within the NHS App is held within the Azure hosted environment. It is stored within the following data repositories:

- **CosmosDB:** Holds the following data –
  - User, info, devices & session information for access into the NHS App
  - Notification and message details
  - Audit information in the event of legal challenges
- **Databricks / FDP:** Holds the analytical data on how the NHS App is being used[12]
- **Splunk:** Holds the log monitoring information that allows for errors within the NHS App and its environment to be investigated

Sources of data

Personal data processed by NHS App Services will be provided:

- by the data subject (the user)
- by the GP practice system
- via user research form input
- via linked profiles (proxy)
- by the NHS Trust system
- by NHS commissioned organisations sending messages via NHS App Messaging and NHS App Notification services

[11] N.B. While the NHS App processes this operational data, including personal data items, the content of connected services, e.g. GP health records remain securely stored within NHS central systems. The app does not permanently store user health records on their device; instead, it provides a secure interface for accessing them.

[12] And will then transition into the NHS Federated Data Platform from 2025 https://www.england.nhs.uk/digitaltechnology/nhs-federated-data-platform/

- by NHS England Systems[13]

Method of data retention and deletion
• Audit, Session and Messaging data is retained in the CosmosDB repository in alignment with the NHS Records Management Code of practice. For messaging data, sending organisations will retain copies of their communications according to their own data retention policies • Performance data is retained on Databricks (transitioning to the NHS Federated Data Platform during 2025) • Data is deleted automatically once their respective retention periods expire using automatic scripts Further information on retention periods is available in section 12
Level of 'High risk' processing
No high-risk processing is performed on the data stored within the NHS App The NHS App will provide an Access Point to Personal Medical Records via the Public Internet. The Inherent Risk Levels has been assessed against the NHS Data Risk Model – the output presented a data Class of V. As such, the processing of data for NHS App has been considered in line with the security controls[14] required to meet the NHS Data Class model of Class V. In addition, data processing activity does not include any of the following: • Large-scale profiling • Automated decisions made by AI or algorithms using the data stored within the NHS App • Sensitive data – The NHS App connects to NHS Login, which contains sensitive ID verification data (but no medical or health data) • Systematic monitoring • Use of AI or machine learning • Data concerning vulnerable subjects[15]. User data does not contain any data of users who are under-13 or any data to identify a vulnerability.

[13] E.g. NHS Login, NHS Wayfinder, NHS Notify

[14] Board level organisational commitment, following specialist advice and guidance due to the data being at the highest level of risk – Cloud Centre of Excellence Good Practice;

[15] The Information Commission Office (ICO) published guidance on 'vulnerable individuals' in the context of data sharing - When do we need to do a DPIA? | ICO

Scope of processing

<table>
<tr><th>Nature of the data</th></tr>
<tr><td>Overview and frequency[16] of data collection</td></tr>
<tr><td>Presentation and transmission layer for services controlled by other data controllers (e.g. GP Practices, NHS Trusts)</td></tr>
<tr><td>The NHS App functions primarily as a user interface allowing users to access a range of healthcare services. While it does not directly store or maintain clinical records. It processes personal data by:

• Collecting and transmitting user inputs to backend services (e.g. via NHS Login and GP Connect APIs)
• Displaying health and care information retrieved from authorised systems

This data is collected continuously while users log into and access services via the App based on the services they access.</td></tr>
<tr><td>Outright data controller/processor for data generated by the App's operation (see below)</td></tr>
<tr><td>The NHS App maintains and stores only the following types of data to ensure its functionality and improve user experience. This includes:</td></tr>
</table>

Type of data	Frequency of collection
Audit Data: Information about user activities within the app, such as the time of use and actions taken, is captured against the user's NHS number.	Data is collected when a user performs an action within the NHS App. It is continuous in nature
Messaging Data: The content of messages sent and received through NHS Notify and viewed using the App's messaging service.	Data is collected when a user receives a message. It is continuous in nature.
Performance Data: Technical data about how the user interact with the app, including device information and usage patterns. [17]	Data is collected when a user makes use of the NHS App. It is continuous in nature

[16] The NHS App has collected data on an ongoing basis since September 2018.

[17] Adobe Analytics supports detailed analysis of consented interactions and journeys within the NHS App; Databricks/FDP supports the separate production of aggregated operational analytics, dashboards and planning information.

Session Data: Temporary information stored during the use of the app by a user such as session cookies.	

Further information on the personal and special category data items processed by the NHS App can be found in section 8 of this document.

Amount of data processed

As at March 2025, the NHS App has accumulated a data collection size of approximately 40 terabytes of data since its inception. This considers the respective data retention periods for audit, messaging and performance data which are set out in section 12 of this document. This will continue to grow based on App user activity as described in the sections immediately above and below.

Number of individuals affected

The platform's total user count exceeds 32 million users[18] and continues to grow at over 200,000 new users each month[19]

In terms of active users, NHS App usage varies from month to month. NHS England has reported that the App was used actively by 12 million people during March to May 2024, 2.3 million aged 66 and over[20]

Geographical area covered

The NHS App can be accessed from any country in the world as it can be downloaded on any phone with an Apple ID or Google Play account that is set to 'UK'[21] or internationally via the web browser (desktop).

To use the App users must

- Fall within the age range (see below)
- Be registered with a GP in England or a location that commissions the NHS App use in their administrative areas (e.g. the Isle of Man)[22]
- Verify their identity. Verification methods may require SMS verification to a UK number
- Local restrictions in some regions outside the UK may affect NHS App functionality[22]

Age range included

[18] The total number of P9 verified users of the NHS App crossed over 32 million in February 2025
[19] Based on data up to November 2024. December 2023 was the most recent month which recorded fewer than 200,000 New NHS App sign-ups (which includes both P5 & P9)
[20] https://www.england.nhs.uk/2024/08/libraries-supporting-more-people-to-use-nhs-app/
[21] In general, this will be the default for UK devices, but this setting can be changed in a user device's settings. The NHS App may be available in App stores for other countries – in this case the user may not need to change their device's region settings to download it.
[22] Local services in Scotland, Wales or Northern Ireland don't fully support NHS App services, so would limit usability.

The service is for users who are 13 years of age or older. For users between the age of 13-15, an approval is required from a GP practice as the Controller of personal data contained in a GP record. This is required to approve access to GP online services via the NHS App.

5. Describe the legal basis for the processing (collection, analysis or disclosure) of personal data

NHS App - England
Statutory Vires
Under section 254 of the Health and Social Care Act 2012 and Regulation 32 of the NICE Regulations[23], the Secretary of State for Health and Social Care has directed NHS England to provide the NHS App Services: NHS App Directions 2023 - NHS England Digital
Legal bases: Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR)
Personal data • UK GDPR Article 6(1)(a) - 'consent of the individual' for those who wish to use the NHS App and for the purposes of non-essential cookies (which comprise personal data) which are placed on the platform. • UK GDPR Article 6(1)(c) – the 'processing is necessary for compliance with a legal obligation to which the controller is subject' – namely, in order to comply with the terms of the NHS App Directions 2023 - NHS England Digital **Special category data** • UK GDPR Article 9(2)(g) – 'processing is necessary for reasons of substantial public interest' and/or • UK GDPR 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, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services' and/or • UK GDPR Article 9(2)(i) - processing is necessary for reasons of public interest in the area of public health and • Data Protection Act 2018, Schedule 1, Part 1, Paragraph 2(2)(f) – 'the management of health care systems or services or social care systems or services'.
Common Law Duty of Confidentiality
The common law duty of confidence is also met as there is a statutory basis for data collected under the above direction, for both directing and directed organisations. For the services provided by health care organisations (e.g., GPs) on the NHS App, where confidential patient data is shared, this is done at the direction of the healthcare organisation for direct care purposes based on implied consent of the patient. NHS England collects data for audit purposes as directed under the NHS App Directions 2023.

[23] National Institute for Health and Care Excellence (Constitution and Functions) and the Health and Social Care Information Centre (Functions) Regulations 2013

NHS App – Isle of Man

The NHS App is available to use by those users registered with a GP in Isle of Man. Access may need to be activated by a patient's GP. The Service to Isle of Man users is provided under a request from the Isle of Man Government using their legal powers under the National Health Service Act 2001 (an Act of Tynwald) (NHSA 2001).

By way of further information on how the Isle of Man health care provision is provided, Manx Care is a statutory board of the Isle of Man Government established by order pursuant to section 12 of the Manx Care Act 2021 (an Act of Tynwald). It is the duty of Manx Care to exercise its powers to discharge the functions of the Department, including, including the duty to promote in the Isle of Man a comprehensive health and social care service.

In accordance with a mandate between the Department and Manx Care, the Department may mandate that Manx Care discharge the Department functions regarding this Information System.

NHS England undertakes provision of the NHS App service under section 270 of the Health and Social Care Act 2012 (the 2012 Act) and in relation to the collection and dissemination of data necessary to provide the service, under section 255(1) of the 2012 Act. Isle of Man Department of Health and Social Care access to the NHS App – NHS Digital

NHS Wayfinder Services Directions 2023

Data collected for the purpose of providing the NHS Wayfinder Service is covered by a separate Legal Direction. The Direction is located here – NHS Wayfinder Services Directions 2023 – NHS England Digital

NHS Notify Service Directions 2025

Data collected for the purpose of providing the NHS Notify Service is covered by a separate Legal Direction. The Direction is located here – NHS Notify Service Directions 2025 - NHS England Digital

COVID-19 Public Enquiry[24]

Statutory Vires

- Covid-19 Public Enquiry
- Inquiries Act 2005

UK GDPR and Data Protection Act

- UK GDPR Article 6(1)(c) – *the 'processing is necessary for compliance with a legal obligation to which the controller is subject'* – namely, in order to comply with the terms of the NHS App Directions 2023 - NHS England Digital

[24] In March 2022, the Government announced that there will be a COVID-19 Public Inquiry, the associated draft COVID-19 Inquiry Terms of Reference includes NHS App within its scope.

- UK GDPR Article 9(2)(g) – '*processing is necessary for reasons of substantial public interest' and/or*
- Data Protection Act 2018, Schedule 1, Part 2, Paragraph 6 – *'statutory and government purpose'*

Common Law Duty of Confidentiality
The common law duty of confidence is also met as there is a legal obligation and a legal hold on deletion for the purpose of the public inquiry.

6. Demonstrate the fairness of the processing

Data items
The NHS App processes only the data necessary to provide its services, adhering to principles of data minimization and purpose limitation. • The NHS App accesses data strictly relevant to the services, improving functionality, resolving technical faults, maintaining and improving security, complying with the law and protecting users against potential fraud. Data is not collected for marketing purposes[25]. • Data is only retrieved from NHS systems when a user actively chooses to access it (e.g. viewing medical records, ordering a repeat prescription). • The NHS App uses digital APIs with filtering logic, designed to serve only necessary fields per use case. (e.g. A prescription API will return current medication info, but not full historic pharmacy records unless explicitly requested, A user's record of historic GP appointments will only display the last 2 years, unless explicitly requested). • The NHS Number is used solely as a unique identifier within the system and is not linked with healthcare attributes for profiling or unrelated purposes. (set out in section 8). Further information on how user data is used is available in the NHS App Privacy Policy.
Lawful basis
All data processing is conducted under a lawful basis in line with UK GDPR. (set out in section 5).
Security
The NHS App's makes use of robust security measures to ensure smooth operation and data security (set out in section 14).
User rights
Users rights regarding their data, including access, rectification, and objection (set out in section 13).

[25] In exceptional circumstances, information suggesting the user or others may be at harm may be used

7. Ensuring individuals are informed about the ways in which their personal data is being used

Privacy Policy
The NHS App privacy policy provides the details of all processing. This is updated regularly, and past copies are available to show the progression of the Policy. NHS App privacy policy - Version 6.5 - NHS (www.nhs.uk) There are also additional privacy policies for core NHS app services: • NHS App privacy policy: online consultation services • NHS App privacy policy: personal health record services • NHS App privacy policy: messaging services Other related services Privacy Policies can be found here: • NHS login: Your Privacy on NHS login • NHS Wayfinder: NHS England » NHS Wayfinder services • NHS Notify: NHS Notify transparency notice - NHS England Digital
Terms of Use
The NHS App terms of use clarify for users: • The distinction between Core Services and Platform Services and provides links to the relevant privacy policies which set out in more precise terms how data in relation to services and functions is being use. A summary of these is set out at Annex A for reference. • That they may stop using the NHS App at any time, how to cancel their account and that (if they cancel their account) any personal data held will be dealt with in accordance with the data retention policy set out in the privacy policy
Cookies Policy
The NHS App cookies policy clarifies for users: • The types of necessary cookies put on their device, the purpose for doing so (including data implications) and when they expire. • The types of optional analytic cookies put on their device, the purpose for doing so (including data implications) and when they expire. • That if they are using a public computer to access the NHS App (desktop version) they should log out of their account, delete downloaded records and delete cookies from the web browser.

Third Parties

Third party obligations in relation to transparency are defined in the contractual documentation relevant to the service or product provided for the NHS App. NHS England requires each of its third parties to:

- Only use data as instructed
- Process data in accordance with UK GDPR requirements
- Ensure their privacy information is clear and accessible
- Ensure they have implemented the appropriate security measures

Promoting the right to object/Opt out

National Data Opt-Out

NHS App users may opt (via an in-app feature) to have their data excluded from processing used for research or planning. Further information about the NDOO

can be found at National Data Opt-Out - NHS England Digital (digital.nhs.uk).

8. Is it necessary to collect and process all data items?

Justification for the collection and processing
The Platform only processes data sets which are required to deliver the platform, connected services, and services which have been on-boarded by NHS England. The Service desk only processes data sets which are required to resolve issues raised by platform users. The table below gives an account of the reasons for NHS England processing the items of personal data specified above and a full list of data items within the NHS App Master Data Specification.

Data categories	Justification
Name	Basic Patient and User Identifier/Contact Information Displayed on main menu when user logs in and in the Personal Medical Record retrieved from their GP and other NHS services. Retrieved from NHS Login to allow users to log into the NHS App. Required to enable consultations and file downloads. Required for Service Support Desk Collection to contact the user to resolve their issue.
Address	Basic Patient and User Identifier/Contact Information Displayed on the Personal Medical Record retrieved from their GP and other NHS services. Required to personalise services based on geolocation, increasing relevance and efficacy of services for Users. Required for some services to deliver items to User.
Postcode	Basic Patient and User Identifier/Contact Information Displayed on the Personal Medical Record retrieved from their GP and other NHS services. Required to personalise services based on geolocation, increasing relevance and efficacy of services for Users. Required for some services to deliver items to User.
Home Phone Number	Basic Patient and User Identifier/Contact Information Displayed in user's contact details in their account settings menu if it is

Data categories	Justification
	part of the details their GP or other NHS services use to contact them. Required for Service Support Desk Collection to contact the user to resolve their issue.
Mobile Phone Number	Basic Patient and User Identifier/Contact Information Displayed in user's contact details in their account settings menu if it is part of the details their GP or other NHS services. Retrieved from NHS Login to allow users to log into the NHS App (authentication). Required for Service Support Desk Collection to contact the user to resolve their issue. Required to support notification and messaging campaigns.
Email Address	Basic Patient and User Identifier/Contact Information Displayed in user's contact details in their account settings menu if it is part of the details their GP or other NHS services. Retrieved from NHS Login to allow users to log into the NHS App Required to enable consultations and file downloads. Required for Service Support Desk Collection to contact the user to resolve their issue.
Date of Birth	Basic Patient and User Identifier/Contact Information Displayed on the Personal Medical Record retrieved from their GP and other NHS services Required to enable consultations and file downloads.
Age	Not displayed in the NHS App Required to support analytics and provision of management information and dashboards
Sex	May be displayed on the Personal Medical Record retrieved from their GP and other NHS services. NHS England does not have control over the content.[26]

[26] Accelerated access to GP-held patient records 2023: From 31 October 2023, practices are contractually obligated to provide online records access for their patients including the coded record and any associated free text, records of consultations along with any associated free text, all test results and all documents.

Data categories	Justification
	Does not transit the NHS App infrastructure, and therefore is not retained by NHS England for the purposes of the NHS App
Gender	May be displayed on the Personal Medical Record retrieved from their GP and other NHS services. NHS England does not have control over the content.[26] Does not transit the NHS App infrastructure, and therefore is not retained by NHS England for the purposes of the NHS App **Error! Bookmark not defined.**
NHS Number	Basic Patient and User Identifier/Contact Information Displayed on main menu when user logs in and in the Personal Medical Record retrieved from their GP and other NHS services. Required for Audit Tracking and within the analytics pipeline. Required to enable consultations and file downloads. N.B. In the case of a proxy managing another user's health on their behalf (e.g. a parent managing a child's healthcare): • The NHS number of the intended beneficiary (e.g. the child) which will be processed beyond the Login process. The NHS number of the proxy (e.g. the parent) is only processed during Login
Registered GP ODS code	Required to produce Management and statistic information at a level which does not disclose personal information or directly identify an individual.
ODS codes of sending services	Required by the NHS App Messaging Service to uniquely identify the sending service as well as look up information related to that service such as the service's name.
Physical Description	May be displayed on the Personal Medical Record retrieved from their GP and other NHS services. NHS England does not have control over the content.[26] Does not transit the NHS App infrastructure, and therefore is not retained by NHS England for the purposes of the NHS App
Behavioural Data – NHS App usage	Required to incrementally improve and personalise NHS App user experience by building and understanding of how an individual has engaged with the NHS App.
Special category data	

Data categories	Justification
Personal Medical Record	Transmission of medical information that has been clinically authorised for a patient to view, including letters, test results and record extracts between healthcare professionals and patients to support patient care. This is extended to file uploads, where patients may wish to upload an image to support a consultation, appointment, booking and referral letters. The App will also support patients with sharing medical information with NHS services.
Messages from health and care providers (via NHS Notify)	Messages processed as part of NHS App Messaging and NHS App Notification Services will persist within the NHS App repositories
Physical / Mental Health or Condition	Maintained as part of the Personal Medical Record. Patients will have the opportunity to view this data via the NHS Online App.[Error! Bookmark not defined.] Does not transit the NHS App infrastructure, and therefore is not retained by NHS England for the purposes of the NHS App
Electronic Prescription Services (EPS) data	
A count of prescriptions returned for that patient and for each prescription. A full list of EPS data items is set out in the Master Data Specification	Through integration with the EPS Prescriptions for Patients API, these data items are sent from Spine to the API Platform and to the requesting NHS App session for all active prescriptions matching a specified NHS number. Necessary to provide prescriptions information and a digital barcode which patients can use to collect a prescription at a pharmacy of their choice. Functionality to allow a patient to track the status of their prescription is being introduced. Patients can track their prescription at an item and prescription level, The prescription level status is formulated from the combination of item level statuses received from EPS.

9. Describe if personal datasets are to be matched, combined or linked with other datasets (internally or for external customers)[27]

NHS App
• To investigate and diagnose faults where a use is using the NHS App and NHS login, the NHS login ID is used as a unique Identifier, along with the NHS number. • For analytics and performance management of the NHS App service. The NHS number is used as a unique identifier. NHS England will assimilate management information from the NHS Number, ODS Code and activities such as the number of appointments booked and other management information requirements. However, the management information will not include any personal information but is created from personal information as the source. • Data may be linked to other datasets for the purpose of dissemination/publication, management information reporting and internal analysis. This will be done for the purposes of monitoring NHS App usage and understanding user behaviour to improve the product offering. This linkage will only occur where approved by information governance team and in accordance with information governance procedures and controls, including where required, advice from the Advisory Group for Data.
NHS App Notification and Messaging Services
To deliver the NHS App Messaging and NHS App Notification Services: • The NHS numbers of message recipients are mapped to the NHS login IDs associated with that NHS Number • The ODS code of the Sending Service is validated using the central ODS Service

[27] Where data may be linked for the purposes set out below, this will be subject to the DPIA being updated to provide details on the linkage and assess any associated risks.

10. Describe if the personal data is to be shared with other organisations and the arrangements you have in place

Personal data is shared between NHS services such as NHS Login, The NHS API with other organisations depending on the service being accessed by the user via the NHS App

The NHS App serves as a secure access channel to services provided by multiple organisations across the NHS. Data sharing is function-specific and for direct care purposes only. See breakdown below of use cases for how data is shared with primary and secondary care organisations and integrated third parties[28].

User action	Data shared	Source[29]	Destination	Data controllership
Primary Care				
Book GP appointment	NHS number, selected slot, patient name/contact	NHS England's API Gateway	GP system	GP practice (C), NHS England (P)
Order repeat prescription	NHS number, medication requested, contact info			
Access GP record	NHS number, request for record segments			
Send message to GP	NHS number, message content	NHS App (direct) or 3rd party integration		GP practice (C), NHS England or 3rd party integration (P)
Secondary Care				
View Hospital Appointment	NHS number, auth token, booking metadata	Wayfinder (hosted by NHS England)	Hospital system	Hospital Trust (C), NHS England (P)
Send message to Hospital	NHS number, message content	3rd party integration		Hospital Trust (C), 3rd party integration P)

[28] For services such as organ donation, national data opt-out preferences, NHS login, general app usage, personal data is shared between the user and NHS England directly

[29] All sources act on user input in the NHS App which initiates a secure request routed via NHS England's backend systems (in general via the NHS API gateway) to the relevant service (e.g. user's GP/hospital system)

Arrangements in place
GP Practices (Primary Care
To deliver NHS App services relating to primary care (e.g. book GP appointments, order repeat prescriptions and view health records) the following information is shared between NHS England's API gateway and GP systems (via the NHS App): • NHS number, details of the request, and contact info if applicable (appointments, prescriptions). • Governance: ○ Data sharing agreements (DSAs) between NHS England and GP practices via GP Connect Onboarding   ○ The GP Connect National Data Sharing Agreement outlines the data sharing requirements and obligations for the use of GP Connect
NHS App Notification and Messaging Services
To deliver the NHS App Messaging and NHS App Notification Services the following information is shared: • The Sending Service, and if appointed, a 3rd party Communication Supplier (including NHS Notify[30]) will have access to the NHS Numbers of patients at a given GP Practice who have registered for the NHS App and if they have Notifications enabled. • The Sending Service, and if appointed, a 3rd party Communication Supplier will have access to the delivery status of the messages they have sent • They can only see the status of messages they have sent and not messages sent by other Sending Services / 3rd party communication suppliers
NHS Wayfinder (Secondary Care)
In order to deliver the NHS Wayfinder service the following information is shared. • NHS Numbers will be shared with Patient Aggregator to enable the tracking of a user through the Wayfinder journey for the purpose of service delivery improvement and optimisation, monitoring, business case and benefits case measurement and wider dissemination as needed.

[30] This messaging platform across NHS England is used across the NHS App, SMS, email messages and letters for campaigns (e.g. vaccinations, screenings, referrals etc). https://notify.nhs.uk/

11. Describe how long personal data is retained

Category of information	Retention method	Retention period
NHS App data used for audit purposes[31]	Stored in the NHS App Production Audit Database (Cosmos)	**Up to 8 years** (in line with the NHS England Retention Policy and NHS login) to ensure correlation between NHS App and NHS login.[32]
NHS App transactional data used for analytical purposes	Stored in the NHS App Production Analytics Database (Databricks)	**Up to 8 years** (in line with the NHS England Retention Policy and NHS login) to ensure correlation between NHS App and NHS login.[33] For further information on how this data is used for analytical purposes by the NHS Federated Data Platform (FDP) please see the NHS App Analytics National FDP DPIA. Data of this kind relating to features that become defunct are still retained for a period of **12 months** to support continuity of data quality in aggregated analytics summaries.
	Stored on Adobe Analytics Servers	**Up to 24 months** For further information on how this data is used for analytical purposes, please see the National Digital Channels Adobe Analytics Cross Channel Tracking DPIA
NHS App service desk information	Stored in ServiceNow with controlled access.	**Up to 12 months**
NHS Login data	Stored in NHS Login systems not within the NHS App	**Duration of the user's lifetime** with the NHS Login service. This is to support analytics and provision of management information and dashboards.

[31] Auditable data refers to any personal identifiable information or event which may be used to support an investigation or review performance management within the NHS App which relates to the user activity or information processed on behalf of the user
[32] Unless an investigation is current at the expiry of the 8 years
[33] Unless an investigation is current at the expiry of the 8 years

		If an app user deletes their NHS login account, the data will be retained for 12 months. Further information is available in the NHS Login DPIA.
NHS App Messaging and NHS App Notification Services data	Stored in the NHS App Notifications and Messages Database (Cosmos)	**Duration of the user's lifetime** with the NHS Login service. This is to offer Citizens / Patients / NHS App Users a like for like service with existing channels (e.g. emails / SMS from sending services) If an app user deletes their NHS login account, their NHS App messages will be deleted, and they will no longer be able to access or retrieve them.
NHS Patient Aggregator (Wayfinder)	Stored in NHS Wayfinder Aggregator systems not within the NHS App.	Data related to the use of NHS Patient Aggregator (Wayfinder) may be held in accordance with the terms set out in the NHS Patient Aggregator DPIA.

The COVID-19 Public Inquiry (announced March 2022), the associated draft COVID-19 Inquiry Terms of Reference includes NHS App within its scope. Therefore, the key personal data will be held in identifiable form in archive for as long as it is considered necessary to meet the needs of the Public Inquiry, as it is considered that this access may be necessary to support queries from the Public Inquiry.

12. Where you are collecting personal data from the individual, describe how you will ensure it is accurate and if necessary, kept up to date

NHS App
• The Service desk information is provided by the data subject, as such, NHS England relies on the Data Subject's assertion that the information they provide is accurate. NHS England will only be able to update this information if the data subject updates NHS England requesting the changes to the data held. • Age is used to support analytics and provision of management information and dashboards is provided by the data subject, as such, NHS England relies on the Data Subject's assertion that the information they provide is accurate. NHS England will only be able to update this information if the data subject updates NHS England requesting the changes to the data held. • The Audit data and NHS Number is collected via a transaction between NHS login and the GP System, as such NHS App will be able to automatically update its record of the NHS number held for the data subject constantly. • The performance data is dependent on the cookies used by NHS App. This is kept up to date by requesting user action when there are changes to the cookie policy.
NHS App Notification and Messaging Services
NHS App Messaging and NHS App Notification Services has no personal information that needs to be maintained for the purpose of accuracy.

13. How are individuals made aware of their rights and what processes do you have in place to manage such requests?

Users may have a legal right under the Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulation (UK GDPR) to:

- know how and why their data will be collected, processed and stored
- request a copy of their personal data
- request corrections to errors or omissions in their personal data
- request to restrict our use of their personal data (e.g. if it's inaccurate and needs to be corrected)
- request to have data deleted

Further information is provided in the NHS App Privacy Notice

Users exercise these rights by:

1. Making a Subject Access Request (SAR) to NHS England's Information Rights Request team via england.irr@nhs.net.
2. Requests will be considered under the DPA 2018 and UK GDPR and responded to on a case-by-case basis.
3. Unresolved queries or concern can be escalated to the Data Protection Officer via england.dpo@nhs.net

14. What technical and organisational controls for "information security" have been put in place?

NHS England

The NHS App service has completed assurance requirements set by NHS England.

- Technical and Organisational controls for Information Security have been considered for the NHS App Project and the service has been considered within a 'Privacy by Design' and 'Secure by Design' approach.
- NHS App uses the corporate risk tool to manage risks identified as part of the risk assessment process.
- System Level Security Policy (SLSP)[34] has been completed and is updated every 6 months.
- A registered penetration test of the service is performed on a yearly basis (last performed Oct 2024).
- Processes are in place to manage and improve the security posture and address any security debt and security related findings
- There are two CSPs in the NHS Solution; the data flow is captured in the data trace within this document:
- The NHS App solution is hosted by a Cloud Service Provider and located within UK only.
- A third-party cloud security solution provides Web Application Firewalling (WAF) of all inbound Internet sessions. The nature of the WAF service requires the encrypted data to be decrypted and inspected as part of the service, and this provides a protective control against malware and Distributed Denial of Service and then re-encrypts the traffic to send to a supporting service, Site Shield. The traffic is then sent to the hosting service, which ensures the traffic into the NHS App is from a group of known 'whitelisted' Site Shield endpoints.
- NHS England is registered in the Data Security Protection Toolkit (DSPT) achieving standards met or exceeded. It publishes its assessment annually (latest July 2024)

Third parties

The NHS App is operated by suppliers who provide digital outcomes and technical solutions to support the programme. These suppliers are bound by UK GDPR compliant contracts, and their services are procured from catalogues such as Digital Outcomes and Specialist (DOS), part of the Crown Commercial Service (CCS) Framework. Each supplier must also:

- Complete the NHS England onboarding process, which includes the relevant security training
- Hold a Valid Data Security and Protection Toolkit (DSPT) assessment achieving standards met or exceeded. A DPST assessment must be done every 12 months.
- Adhere to the standards and security best practice requirements outlined in the contract and that have been set out by NHSE.

[34] This is foundational document outlining the security requirements, responsibilities, and controls for a particular system or set of systems. Including strong access controls and data security controls. The SLSP. Further details on security concerning specific NHS App services (e.g. NHS App Notification and Messaging Services) are detailed in the SLSP

- Suppliers are required to participate in assurance activities that relate to the security of the service.

Suppliers must demonstrate compliance against various industry recognised and NHSE defined technical policies and standards.

15. Where personal data is stored or processed[35]

The programme engages a range of third-party suppliers, which fall into two primary categories:

- **Backend Suppliers:** These are organisations that support the infrastructure, security, operations, and delivery of the service. This includes (but is not limited to):
- **Frontend Integration Suppliers:** These are suppliers whose products and services are directly integrated into the user-facing application, enabling end users to access specific health or administrative functions. This includes (but is not limited to):

At present, the programme works with:

- Over 20 backend suppliers, all of which are based in the UK or EEA
- Over 20 frontend integration suppliers, all of which are also based in the UK or EEA

All suppliers are Further details, including supplier names, functions are set out in Annex D

[35] All approaches to data processing are governed by contractual agreements between NHS England and the supplier.

16. Identification of Risks and Measures to control/mitigate (treat)

Risk scope
This document focuses on cross-cutting privacy risks arising from how the NHS App processes personal data. It includes risks that, as a result of the design, operation, or intended use of the NHS App and its connected services, could **directly** lead to: 1. a personal data breach and/or 2. Non-compliance with UK data protection law or regulatory requirements. All risks identified in this document are subject to ongoing review as part of the programme's wider risk management arrangements.
Operational incidents and subsidiary risks
The NHS App programme also manages operational risks and issues that may increase the likelihood or impact of these aforementioned privacy risks in specific areas (e.g. identity management, account behaviour, cyber-security controls, or clinical workflows). These operational risks/issues are managed through specific NHS App team risk registers and assurance processes (e.g. clinical safety or cyber-security team registers). Therefore, they do not appear in this document. All risks identified in specific NHS App team risk registers are subject to ongoing review as part of the programme's wider risk management arrangements. As part of this, teams are kept informed of the risks in this document, and any material changes. Where teams identify any operational risks in specific registers that may affect the likelihood or impact of a privacy risk described in this document, this information is escalated to the Information Asset Owner and considered as part of regular DPIA risk reviews.
NHS England Risk Scoring Matrix and Guidance
Risks in this document are scored using the NHS England Risk Scoring Matrix and guidance. They are evaluated by combining estimates of impact (also described as consequence) and likelihood (frequency or probability). The score or magnitude of a given risk is established using a two-dimensional matrix, with impact as one axis and likelihood as the other.

	Very minor	Minor	Moderate	Significant	Severe
Highly likely	5	10	15	20	25
Likely	4	8	12	16	20
Possible	3	6	9	12	15
Unlikely	2	4	6	8	10
Highly unlikely	1	2	3	4	5

	Low risk (1-6)
	Moderate risk (8-10)
	High risk (12-16)
	Extreme risk (20-25)

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
1	Technical Measures **As a result of** evolving cyber threats, legacy system integration and potential gaps in continuous security monitoring **There is a risk** that insufficient technical controls are in place to ensure the security and integrity of NHS App data. **This could result in:** 1. A data breach involving NHS App systems which could then lead to 2. regulatory investigation, reputational harm, and a loss of public trust in NHS App digital services. **Type of Risk** Operational (tech security)	Extreme (20)	**Existing controls** The NHS App service has completed assurance requirements set by NHS England. This is set out in full in section 14 of this document. Summary below: 1. Annual penetration test of the service (last performed Oct 2025) 2. The NHS App uses two Cloud Service Providers for enhanced resilience and risk mitigation through segmentation: a. The NHS App solution is hosted by a Cloud Service Provider and located within UK only. b. A third-party cloud security solution provides Web Application Firewalling (WAF) of	Treat	High (12)	[redacted] Head of Delivery (NHS App) 02/05/2025	Controls in place are deemed adequate based on current assessment but must be maintained via BAU

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
			all inbound Internet sessions. 3. Where the NHS App stores data (i.e. audit, session etc databases), access controls are utilised and data is encrypted.				
2	Organisational Measures **As a result of** complexity of third-party arrangements, difficulties embedding organisational governance frameworks, and inconsistent implementation of training and policies. **There is a risk** that organisational measures (e.g. training, governance, supplier oversight) are insufficient to safeguard NHS App data. **This could result in**	**High (16)**	**Existing controls** The NHS App service has completed assurance requirements set by NHS England. This is set out in full in section 14 of this document. Summary below: 1. Technical and Organisational controls considered within a 'Privacy by Design' and 'Secure by Design' approach. 2. Corporate risk tool to manage risks identified.	Treat	**High (12)**	[redacted] Head of Delivery (NHS App) 22/01/2026	Controls in place are deemed adequate based on current assessment but must be maintained via BAU.

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
	1. Regulatory non-compliance which could then lead to 2. Security breaches, regulatory investigation, reputational harm, service disruption, and erosion of patient trust in NHS England's data governance. **Type of Risk** Legal, compliance and regulatory		3. System Level Security Policy (SLSP) outlining data security and access requirements, responsibilities, and controls. 4. NHS England is registered in the Data Security Protection Toolkit (DSPT) and publishes its assessment annually. Latest publication July 2024 5. Third party suppliers are bound by UK GDPR compliant contracts as outlined in government procurement frameworks. The NHS App Delivery Partner service is procured under the Digital Capability for Health (DCFH) framework which is governed by				

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
			Crown Commercial Service (CCS) Other supplier products are also purchased through approved government procurement routes. Each supplier must: a. adhere to the standards and security best practice requirements outlined in the contract and any data and security schedules; and b. demonstrate compliance against various industry recognised and NHSE defined technical policies and standards such as the Data Security and				

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
			Protection Toolkit (Standards Met – Version 6 – 23-24)[36]				
3	<u>Internal bad actors (accidental misuse of data)</u> **As a result of** human error, insufficient understanding of data handling procedures, or failure to follow established operational or security protocols. **There is a risk** that internal staff or contractors unintentionally compromise NHS App data while carrying out legitimate duties. **Which could result in**: 1. A breach of data confidentiality, integrity, or availability through	**High (16)**	**Existing controls:** 1. Data Security Awareness Training completed by all NHS England and supplier staff. 2. Established Joiners–Movers–Leavers process ensuring role-appropriate access and timely deprovisioning. 3. Segregation of duties and role-based access control within NHS App environments. 4. Quarterly review of user access permissions and audit trails.	Treat	**Moderate (8)**	[redacted] Head of Delivery (NHS App) 22/01/2026	Current controls provide a strong baseline for preventing and detecting accidental misuse. Periodic audits and awareness training maintain compliance. Residual risk considered **low to medium**, driven mainly by potential for human error despite mitigations. Given the residual risk depends heavily on human behaviour, should additional controls (e.g. periodic

[36] Set out fully in section 14 (summary: complete the NHS England onboarding process, hold a Valid Data Security and Protection Toolkit (DSPT), participate in assurance activities that relate to the security of the service).

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
	mishandling, misdirection, or inappropriate access to NHS App data, which could then lead to 2. Regulatory investigation, reputational harm, user complaints, and a loss of confidence in NHS App's internal data governance. **Type of Risk:** Operational (tech security)		5. NHS England ICT standards for supplier hardware and endpoint protection. 6. Incident reporting and root-cause analysis process for near-misses or training gaps.				scenario-based refreshers, enhanced audit for high-risk functions) be considered to further reduce likelihood or detect issues earlier?
4	<u>Internal bad actors (malicious misuse of data)</u> **As a result of** motivated individuals exploiting privileged access while bypassing detection, possibly for personal gain, retaliation, or ideological reasons. **There is a risk that** a staff member, contractor, or supplier with legitimate	**High (15)**	**Existing Controls:** 1. Segregation and management of privileged access rights. 2. Personnel security screening (BPSS minimum; SC vetting for critical roles). 3. Monitoring and audit logging for privileged user actions.	Treat	**Moderate (8)**	[redacted] Head of Delivery (NHS App) 22/01/2026	Controls in place are deemed adequate based on current assessment. While strong preventive and detective controls exist, complete elimination of malicious intent is not achievable. Residual risk remains

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
	access intentionally misuses NHS App data. **Which could result in:** 1. A data breach involving unauthorised disclosure, alteration, or exfiltration of NHS App data, which could then lead to 2. Regulatory investigation, reputational harm, loss of public trust, scrutiny over NHS England's internal access controls, and increased pressure for technical and policy reform.		4. Supplier compliance with NHS England ICT and contractual security requirements. 5. Enforcement of Joiners–Movers–Leavers process for timely removal of access. 6. Whistleblowing and misconduct reporting mechanisms to detect malicious intent. 7. Quarterly review of control effectiveness and audit outputs. 8. Security issue log capturing and tracking technical vulnerabilities relevant to insider risk.				**medium**, managed through continuous monitoring, staff vetting, and deterrence measures.
5	<u>Open-Source Code Repositories</u> **As a result of** the publication of components, libraries, or code pipelines	**High (12)**	**Existing Controls:** 1. **Regular scans** are performed of the application code to determine	Treat	**Moderate (8)**	[redacted] Head of Delivery	Controls in place are deemed adequate based on current assessment.

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
	used in building or running the NHS App. **There is a risk** that a vulnerability in open-source code used by the NHS App is exploited. **Which could result in:** 1. A data security breach, including unauthorised access or compromise of NHS App systems, which could then lead to 2. Reputational harm, loss of public trust in NHS App development practices, regulatory scrutiny, and questions around use of open-source tooling in critical infrastructure. **Type of Risk:** Operational (tech security)		vulnerabilities in the packages and modules. Scanning results are manually checked and remediated if possible. 2. **Static Code checks** are performed during the compilation of the code 3. **Pipeline is monitored internally and includes control gates** to ensure it does not contain significant vulnerabilities.			(NHS App) 22/01/2026	

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
6	<u>Denial of service attack being launched against the NHS App</u> **As a result of** the removal of geo-fencing, increasing its visibility to potential malicious actors. **There is a risk** that a person or organisation may launch a Denial of Service (DoS) attack against the NHS App, exploiting its expanded attack surface. **Which could result in:** 1. A disruption to the availability of the NHS App, including partial or complete service outages, which could then lead to 2. Reputational damage, reduced public trust, delayed access to care services (e.g. appointments, prescriptions), and	**High (16)**	**Existing Controls:** 1. The NHS App uses Akamai WAF and Site shield as their "front door" protection. The capability is set to trigger if a DoS attack is detected and block the incoming traffic from the detected IP Addresses. 2. Logs and configuration regularly reviewed with supplier 3. Rate-limiting and throttling are configured at the API Gateway to prevent excessive authenticated requests from degrading performance; alerting is in place for abnormal usage patterns.	Treat	**Moderate (8)**	[redacted] Head of Delivery (NHS App) 22/01/2026	Controls in place are deemed adequate based on current assessment.

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
	clinical safety risks for patients reliant on timely digital access. **Type of Risk:** Operational (tech security)						
7	<u>Contaminated data via a compromised third-party service provider</u> **As a result of** one of the NHS App's third-party suppliers becoming compromised through an attack or a data breach (the NHS App uses over 30 front and back-end supplier to support functions and features). **There is a risk** that malicious or malformed data is transmitted from a compromised supplier to the NHS App via established API connections. **Which could result in:**	**High (12)**	**Existing Controls:** 1. The NHS App only receives plain text responses from the suppliers therefore no files or special characters are accepted by the APIs. 2. All APIs have been penetration tested before going live. 3. **Suppliers Conformance Assessment List (SCAL)** required confirming the supplier's adherence to security, compliance and technical standards. 4. Suppliers processing data must demonstrate	Treat	**Moderate (8)**	[redacted] Head of Delivery (NHS App) 22/01/2026	Controls in place are deemed adequate based on current assessment.

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
	1. A data security breach or service contamination affecting NHS App performance or integrity, which could then lead to 2. Reputational damage, user disruption, regulatory scrutiny, and downstream vulnerabilities in NHS England's digital supply chain. **Type of Risk:** Operational (tech security)		a commitment to the **Data Security Protection Toolkit**				
8	<u>Third-party data controllership assertion</u> **As a result of** suppliers asserting themselves as data controllers for services integrated via the NHS App, contrary to NHS England's intended data governance model.	**High (12)**	1. **Contracts** with third parties processing data define data-sharing roles (NHS England: Controller, Third-party: Processor) and set out the parameters for data processing by the third-party. 2. **Suppliers Conformance**	Treat	**Moderate (8)**	[redacted] Head of Delivery (NHS App) 22/01/2026	1. Supplier GDPR role assertions to be reviewed by an assurance mechanism ahead of them going live. 2. Ongoing review on a per supplier onboarding request basis.

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
	There is a risk that a supplier independently processes NHS App-related personal data under its own legal basis, contrary to NHS England's controller role and without appropriate agreements. **Which could result in:** 1. Regulatory non-compliance due to unclear or disputed controllership roles, which could then lead to 2. Reputational harm, legal challenge, ICO intervention, loss of data governance assurance, and erosion of public trust in the App's data handling practices. **Type of Risk:**		**Assessment List (SCAL)** required confirming the supplier's adherence to security, compliance and technical standards includes clarity on the supplier's role as data processor 3. **Connection agreements:** Due diligence is carried out to ensure the relevant controls around marketing and NHS England data use is clear 4. **Supplier privacy notice reviews:** All supplier privacy notices are reviewed to ensure they meet NHS England's controller acceptance levels.				

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
	Legal, compliance and regulatory						
9	<u>Third-party data processing/storage location</u> **As a result of** one (or more) of the NHS App's third-party suppliers processing or storing data in a location outside of the UK or the EEA (the NHS App uses over 30 front and back-end supplier to support functions and features) **There is a risk** that NHS App data is being processed outside of NHS England's data processing risk appetite **Which could result in:** 1. Regulatory non-compliance due to cross-border data transfers lacking adequate safeguards,	High (12)	**Recommended Actions** For each supplier where this occurs: 1. Confirm the basis on which NHS England has allowed the third-party to appoint sub-processors. 2. Confirm which of the supplier's sub-processors it is using to process/store NHS App data. For any outside UK/EEA request the use of a different sub-processors so that NHS App data is only processed within the UK/EEA. 3. Confirm options to discontinue the use of the supplier as necessary	Treat	High (12)	[redacted] Head of Delivery (NHS App) 22/01/2026	As per recommended actions

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
	which could then lead to 2. Data security incidents, reputational harm, increased scrutiny from data protection authorities, legal challenge, and potential disruption to services if suppliers must be disengaged or replaced. **Type of Risk:** Legal, compliance and regulatory		4. Update the NHS App Privacy Notice if required				
10	<u>Incorrectly matched or confused records</u> **As a result of** one or more of the following: 1. PDS incorrectly matching records; or 2. Failure in the NHS Login ID verification process; or 3. Incorrect matching carried out by	**High (12)**	**Existing Controls:** 1. This risk is owned by the NHS Login programme, which keeps a detailed record of it. A copy is of the full risk as at 31/03/25 is available at Annex F. NHS Login will implement the	Tolerate	**Low (6)**	[redacted] Head of Delivery (NHS App) 22/01/2026	This risk is owned by the NHS Login programme

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
	primary or secondary healthcare services **There is a risk** that a user is matched to a record which isn't theirs (incorrect matching) or being shown data on a record which isn't theirs (confused records). **Which could result in:** 1. Disclosure of health information to an incorrect patient and a data breach. 2. This can cause distress and inconvenience, particularly if it results in the inability to access services through the NHS App until it is addressed. This in turn leads to compensation claims from affected individuals. **Type of Risk:**		appropriate verification and security controls, subject to prioritisation, to mitigate their risk. 2. NHS App continues to monitor via NHS Login updates and governance process.				

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
	Legal, compliance and regulatory						
11	<u>Direct Marketing – NHS App Messaging</u> **As a result of** sending organisations (e.g. GP practices) using NHS App messaging for communications that cross the line into "direct marketing" without a valid legal basis. **There is a risk that** a message sent through the NHS App is considered unlawful direct marketing under PECR. **Which could result in:** 1. Regulatory non-compliance relating to PECR and data	**Moderate (9)**	**Existing Controls** 1. Completion of assurance documentation including: ○ Supplier Conformance Assessment List ○ Connection Agreement ○ Acceptable Use Policy 2. Quarterly review of assurance document completion by sending services. Last reviewed 14/03/25	Tolerate	**Low (6)**	[redacted] Head of Delivery (NHS App) 22/01/2026	Controls in place are deemed adequate based on current assessment.

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
	protection law, which could then lead to 2. Reputational harm, patient complaints, ICO investigation, and reduced trust in NHS App communications. **Type of Risk:** Legal, compliance and regulatory						
12	<u>App Messaging failures</u> **As a result of** technical failures, system outages or integration issues **There is a risk** that messages sent through the NHS App are not delivered to patients in a timely or accurate manner. **Which may result in:** 1. Disruption to patient communications, such as missed appointment reminders or care	**Moderate (9)**	**Existing controls** 1. The NHS App Messaging Service tracks the delivery status of messages and Sending Organisations and Communication Suppliers can use this information to act on those not delivered, and make the decision to communicate with the patient via other means e.g. fallback	Treat	**Low (6)**	[redacted] Head of Delivery (NHS App) 22/01/2026	Controls in place are deemed adequate based on current assessment.

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
	instructions, which could then lead to 2. Patient confusion or distress, complaints to NHS organisations, erosion of trust in the NHS App, and potential risks to care outcomes in borderline or vulnerable cases. 3. If the error includes potential breaches of UK GDPR principles of accuracy and integrity this could also lead to regulatory non-compliance. **Type of Risk:** Legal, compliance and regulatory Patient safety and quality of care		options such as SMS / email / telephone, etc. 2. The NHS App notification settings have been simplified and are controlled at a device level, including enabling users to manage their push notification settings. 3. Healthcare providers under their duty of care to patients should be utilising follow-up protocols for contacting a patient where a message is deemed important enough that contact needs to be made with the patient, as it is expected that not all patients can or will use digital products.				

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
13	<u>Multiple User Accounts</u> **As a result of** an individual having multiple NHS login accounts verified at P9 level and mapped to the same NHS number **There is a risk** system-generated messages or notifications are sent to a dormant or inactive account instead of the one the individual actually uses **Which may result in:** important communications not being received, resulting in missed care interventions, increased risk to patient safety. There is also the possibility of non-compliance with data protection principles around accuracy and integrity. These immediate impacts will incur	**Low (6)**	**Existing Controls:** 1. Since February 2023, it has not been possible for users to have more than one account that is verified at P9 level. Therefore, this risk could only arise for users who created multiple accounts before this control was implemented, significantly mitigating the level of risk. 2. NHS App continues to monitor via NHS Login updates and governance process.	Tolerate	**Low (3)**	[redacted] Head of Delivery (NHS App) 22/01/2026	This risk is owned by the NHS Login programme.

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
	reputational damage and erode patient trust. **Type of Risk:** Patient safety and quality of care Legal, compliance and regulatory						
14	<u>Responsibility for accuracy of information provided by connected services</u> **As a result of** the NHS App displaying data (e.g. prescriptions, appointments, test results) pulled from connected services, which may provide inaccurate or outdated information. **There is a risk** that the NHS App displays information from a connected service that is not up-to-date or accurate. **Which may result in:**	**High (12)**	**Existing Controls** 1. The NHS App privacy notice advises users that they can report data integrity issues via the NHS App. NHS England maintains a service desk function which allows the user to interact with NHS England or the connected service to report the data integrity issues for resolution. 2. The NHS App utilises interstitial screens	Tolerate	**Moderate (9)**	[redacted] Head of Delivery (NHS App) 22/01/2026	Controls in place are deemed adequate based on current assessment. Further reduction would require control over connected services' data quality, which is not currently within scope.

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
	1. Users relying on incorrect data to make decisions about their care, which could then lead to 2. Patient confusion or harm, complaints to NHS England or the connected service, increased service desk burden, potential breach of data protection principles (accuracy, accountability), reputational damage, and loss of public trust. If harm occurs, this may also lead to legal claims. 3. If the error includes potential breaches of UK GDPR principles of accuracy and integrity this could also lead to		to advise the user when they are leaving the NHS App service, and moving onto a different service 3. NHS App users must agree to the Terms of Use, which includes provision on NHS England's liabilities to users (s10) relating to accuracy or how up-to-date information is that is being provided though services accessed through the app.				

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
	regulatory non-compliance. **Type of Risk:** Patient safety and quality of care Legal, compliance and regulatory						
15	<u>Secondary use of data</u> **As a result of** secondary uses of NHS App data (e.g. for research, service evaluation, or improvement) not being clearly explained to users or drifting from the original healthcare delivery purpose. **There is a risk** that the NHS App is processing personal data in a manner that is incompatible with the original purpose for which it was collected, or is perceived as such by users. **Which may lead to**	**Moderate (9)**	**Existing controls** 1. NHS App Privacy notice provides the user with a clear description of the processing. 2. Any Management Information requested will be subject to IG review and approval. 3. Where data requires a unique identifier, this will be the NHS login identifier which is classed as pseudonymised and can only meaningfully be associated with patient identifiable	Tolerate	**Low (6)**	[redacted] Head of Delivery (NHS App) 22/01/2026	Controls in place are deemed adequate based on current assessment.

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
	1. Users becoming uncomfortable or withdrawing from the NHS App due to lack of clarity or perceived misuse of data, which could then lead to 2. Legal challenges relating to data transparency, reduction in app uptake or trust, reputational damage, and scrutiny over NHS England's data governance practices. **Type of Risk:** Legal, compliance and regulatory		data once referenced within the NHS login system. 4. Any secondary use of data and linking will be subject to a DPIA for this activity and be reviewed by IG. 5. Any dissemination of data will be subject to review from the Advisory Group for Data.				
16	<u>Using shared infrastructure for primary and/or secondary care data features</u> **As a result of** features in the NHS App using existing	**High (12)**	**Existing Controls:** Data is filtered using specific attributes to identify systems and/or services relating to either primary or secondary care	Treat	**Moderate (8)**	[redacted] Head of Delivery (NHS App) 22/01/2026	Controls in place are deemed adequate based on current assessment. N.B. Filtering by Supplier ID and other

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
	shared infrastructure for both primary and secondary care data. If that infrastructure does not properly filter or segregate data streams, the wrong type of data may be exposed or processed by systems not legally permitted to handle it. **There is a risk** that data flows to a part of the system in breach of NHS App legal directions — i.e., primary care data appears in a service not authorised to process it, or vice versa. **Which may result in:** 1. Non-compliance with the NHS App's legal directions due to improper data segregation, which could then lead to 2. A data security breach, regulatory intervention,		data will ensure only correct data can flow through. The use of filtering for attributes such as 'Supplier ID' can filter out data sent through from suppliers, ensuring only the correct level of information is sent through.				attributes mitigates the risk, but infrastructure sharing means controls must be actively maintained. Any change in service architecture requires re-validation.

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
	reputational damage, and loss of public trust in NHS App data controls and legal compliance. **Type of Risk:** Legal, compliance and regulatory						
17	<u>Account compromise via NHS Proxy user</u> **As a result of** a verified proxy relationship established through NHS App **There is a risk** that a legitimate proxy user acts beyond the intended scope of consent (e.g. viewing sensitive information or requesting medication for self-benefit without prompt detection or revocation. **Which may result in:** 1. A data security breach involving inappropriate	**High (12)**	**Existing Controls:** 1. NHS Login Verification: validates proxy relationships and identity at creation. 2. NHS App Integration Controls: adherence to approved NHS Login API and consent requirements. 3. User-Interface Safeguards: clear distinction between personal and proxy accounts;	Tolerate	**Low (6)**	[redacted] Head of Delivery (NHS App) 22/01/2026	• Joint review with NHS Login on proxy consent and revocation assurance. • Develop analytics to flag anomalous proxy activity patterns. • Reinforce in-App prompts reminding users to review proxy permissions. N.B. While identity verification through NHS Login remains

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
	access to or use of another person's health records, which could then lead to 2. Misuse of NHS services (e.g. prescription abuse), public loss of trust in delegated access via the NHS App, ICO scrutiny or enforcement, reputational harm, and challenge to NHS England's role as data controller for proxy-enabled services.		confirmation prompts for key actions; revocation options. In addition, the proxy application service also enables patients to manage what services a proxy can do on their behalf e.g. only manage appointment booking and not order repeat prescriptions or seeing my health record. 4. **Audit Logging:** all proxy activity logged and attributable. 5. **Operational Governance:** joint reviews and change control with the NHS Login programme.				strong, post-creation misuse of a legitimate proxy relationship cannot always be prevented or swiftly detected. Residual risk rated **medium**, reflecting dependency on user behaviour and operational monitoring rather than technical controls.

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
			6. **User Guidance:** in-App messaging on reviewing and revoking proxy access. 7. **Incident Response:** established escalation routes for suspected misuse. 8. NHS App terms and conditions				
18	<u>NHS App legal directions</u> **As a result of** unanticipated delays in the process for updating Legal Directions **There is a risk that** delays to NHS App feature go-live dates occur, or on an exception basis where appropriate, some features/changes go live without fully approved legal direction cover whilst the relevant changes needed to	**Moderate (9)**	Level of risk accepted where it is too late to reforecast go-live dates. As updates to Legal Directions are pending, the window for impact is limited. **<u>Controls</u>** • Process is in place for consulting IG where any changes to data processing are required. This identifies and captures where a legal direction	Tolerate	**Low (6)**	[redacted] Head of Delivery (NHS App) 22/01/2026	Controls in place are deemed adequate based on current assessment.

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
	legal directions are still pending approval. **This may result in:** 1. NHS England operating without a complete legal basis for some new processing activities, which could then lead to 2. Regulatory challenge (e.g. ICO), questions about transparency, public trust erosion, reputational damage, and scrutiny of NHS App governance maturity. Where features are delayed, this could also lead to political and delivery tension. **Type of risk:** Legal, compliance and regulatory		change may be needed. Where a change involves a restricted activity in the current legal directions to be derestricted, it will not be allowed to proceed until a legal direction change is submitted and approved. Where a change does not require derestriction within the existing legal directions, and delaying its implementation would have a detrimental impact on the delivery of services - the IG SME will work with the IAO and change requestor, and will advise whether a reasonable and risk assessed work-around				

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
			can be put in place to allow a feature to go live whilst a legal direction is pending approval. Noting that this will be on an exceptional basis only. Each case will also be risk assessed individually and logged and tracked within this DPIA for transparency until the risk is eliminated. • NHSE is seeking approval of a more streamlined legal direction change process. This will reduce the risk of delays for NHS App changes from **Q3** 2025 (planned). • Prioritisation and co-ordination of activity to optimise and				

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
			streamline approval processed between NHS England and DHSC				
19	<u>Aggregated NHS App data on the NHS FDP</u> **As a result of** Aggregated NHS App analytics data ingested into the NHS Federated Data Platform including small numbers that are not suppressed, such as low-activity patterns or rare events. **There is a risk that** an individual could be re-identified (or inferred) from these small-number aggregates, if viewed in isolation or in combination with other data. **Which could result in:** 1. Anonymised data being classed as personal under UK GDPR due to	**Moderate (9)**	**Existing controls** Aggregated Data ingested into the Product and/or made available via the NHS App analytics dashboard has small numbers included, a risk assessment was undertaken to ascertain if the Data continue to be Personal Data. Whilst small numbers are included/shown, they have been further aggregated at daily/weekly/monthly and therefore it would not be possible to re-identify an individual in the Data or for the output to be linked with other Data which would enable re-identification to the users of the dashboard.	Tolerate	**Low (6)**	[redacted] Head of Delivery (NHS App) 22/01/2026	Controls in place are deemed adequate based on current assessment.

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
	residual identifiability, which could then lead to 2. Regulatory non-compliance, ICO scrutiny, reputational harm, internal audit findings, and questions about the privacy maturity of the NHS App analytics programme. **Type of risk:** Legal, compliance and regulatory		The Data is therefore considered to be appropriately aggregated and anonymous.				
20	<u>Lack of interstitial screens for linked services</u> **As a result of** inconsistent or missing interstitial screens when users are redirected from the NHS App to external or integrated services.	High (12)	**Mitigating actions** 1. Identify all instances where the NHS App links to external services without NHS login or compliant authentication and without user warning (e.g. blue interstitial). 2. Confirm programme-wide defined authentication	Treat	High (12)	[redacted] Head of Delivery (NHS App) 22/01/2026	**As per mitigating actions**

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
	There is a risk that users will not understand that they have left the NHS App environment and may misattribute responsibility for the linked service, or may interact with services that do not meet NHS England's security or authentication standards. **This could lead to:** 1. Increased risk of security breaches (of App users within the linked service) 2. Reputational harm to the NHS App (reduced user trust). Non-compliance with mandatory organisational requirements (e.g. DAPB3051). Possible		standards for any linked service 3. Implement a mechanism to ensure squads/teams consult IG and security SME's earlier in NHS App feature development pipeline (in line with operating model and governance requirements). 4. Implement Blue Interstitial screens consistently and add periodic compliance checks for linked services.				

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
	loss of NHS login stakeholder trust.						
21	<u>Inappropriate handling of patient-identifiable data (PID) via supplier-managed support channels</u> **As a result of** patients, NHS staff, or other users submitting information through supplier-managed channels (e.g. B2B portals, webforms, or other triage tools) **There is a risk that** patient-identifiable data may be: • Submitted without appropriate lawful basis or transparency, • Accessed beyond its intended purpose,	**Moderate (9)**	**Controls** A. Supplier end controls as appropriate including: i) Role-based access control (e.g. PID stored in restricted fields) ii) Appropriate data retention periods iii) Transparency prompts at point of submission iv) Supplier DPIA coverage B. Detailed and devolved risk management for any known instances within NHS England	Tolerate	**Low (6)**	[redacted] Head of Delivery (NHS App) 22/01/2026	Controls in place are deemed adequate based on current assessment.

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
	including accidental or malicious access, • Processed inappropriately or retained longer than necessary, • Not clearly governed under either the NHS App DPIA or the relevant supplier DPIA. **This could lead to:** 1. Regulatory non-compliance which could lead to 2. Security breaches, regulatory investigation, reputational harm, service disruption and erosion of patient trust in NHS						

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
	England's data governance.						
22	<u>Transparency documentation granularity changes</u> **As a result of** the programme significantly increasing the granularity and completeness of internal data documentation (namely the NHS App Master Data Specification) **There is a risk that** internal documentation and associated transparency materials are misinterpreted by users, stakeholders, or regulators as indicating an expansion in the scale or nature of personal data processing,	**Moderate (8)**	**Controls** A. Established and approved lawful bases, purposes, and retention periods for processing. B. The detailed NHS App Master Data Specification improves governance and accountability in the accuracy of transparency materials. C. Other internal transparency documentation, including the content of the DPIA, are aligned to ensure that descriptions of processing are accurate and lawful while remaining	Treat	**Low (4)**	[redacted], Head of Delivery 22/01/2026	1. Monitor complaints, enquiries, and escalations related to data transparency for signs of misunderstanding 2. Use feedback to iteratively improve explanatory language in transparency documents (if necessary) 3. Update DPIA and Privacy Notice in alignment to any future changes

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
	rather than improved record-keeping and governance maturity. This could lead to: 1. Increased complaints, enquiries, or escalations relating to privacy and data use due to surprise or confusion regarding the perceived volume and interconnectedness of data processing 2. Reduced user trust in the NHS App, additional scrutiny from oversight bodies, reputational harm to the NHS App programme		proportionate and appropriate to the intended audience D. The updated NHS App Privacy Notice includes a layered approach and full description of the NHS App Master Data Specification and a link to this document. E. The publication of documentation to promote transparency, which includes the publication of: • NHS App Master Data Specification • NHS App Privacy Notice • NHS App Data Protection Impact Assessment • NHS App Technical Specification				

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
23	<u>Freetext input via NHS App Contact Us portal</u> As a result of citizens submitting enquiries through the NHS App Contact Us portal, which includes a free-text field for describing technical issues. There is a risk that citizens may include patient-identifiable data (PID) or special category information, within the free-text field despite guidance discouraging this. This may result in personal data being inappropriately handled, particularly: 1. Collection where it is not required for the stated purpose of technical support		**Controls** A. Transparency and user guidance: Clear messaging on the NHS App contact form discourages users from including personal or medical information within free-text submissions. B. Secure transfer of submitted information: Data submitted through the contact form is securely transferred via API into the ServiceNow's service desk platform used to manage NHS App support requests. The webform itself does not retain submitted data. C. Sensitive data flagging and access controls:	Tolerate		[redacted] Programme Manager 22/09/2026	Controls in place are deemed adequate based on current assessment.

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
	2. Retention within system records or audit history beyond the intended operational need if not appropriately managed This could lead to: 1. Regulatory non-compliance; and 2. Security incidents, reputational harm, and erosion of public trust in NHS England's handling of personal data.		Cases created from NHS App contact forms are automatically marked as containing sensitive data within ServiceNow. D. Operational redaction process: Where citizens include personal or sensitive information within the free-text field: E. Audit logging: The service desk platform maintains immutable audit history to support operational traceability. Where information is redacted within the case description, the historic audit record may retain the original text. A defined process exists within ServiceNow for				

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
			removal of highly sensitive information from audit history where necessary. F. Retention controls: Support cases are retained within ServiceNow for 12 months following the last communication, unless the case is marked for extended retention where required for investigations or operational purposes. Non-personal metadata may be retained for reporting and trend analysis.				
24	<u>Potential preferential browser recommendation in App pop-up message</u> As a result of an NHS App pop-up message displayed	**Low (6)**	**Mitigating action** 1. Confirm browser testing compatibility – is the recommendation advisory or is access	Treat	**Low (4)**	[redacted] Head of Delivery (NHS App)	**As per Mitigating actions**

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
	to users on starting the App specifically recommending Chrome (Android users) or Safari (iOS users) for the best experience. Stakeholder criticism has already occurred. There is a risk that the popup recommending users install/use Chrome or Safari could be perceived as favouring specific commercial browser providers or steering users towards particular products. This could lead to: 1. NHS England being exposed to legal, commercial, reputational or policy challenge that the service is giving preferential		via other browsers blocked for users 2. Address the pop-up directly if in NHSE's control, either: a. Reword it using neutral browser-support language, providing a justification or technical explanation why specific browsers are recommended; or b. Remove it entirely 3. Obtain Legal/commercial view on the potential impacts.			04/06/2026	

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk	Residual risk	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
	treatment to specific browser providers, restricting user choice or failing to align with public sector expectations around neutrality, open standards, accessibility, or interoperability.						

17. Further Actions

- The completed DPIA should be submitted to the Privacy Transparency and Trust (PTT): Analytics and Operations team for review.

- The IAO should keep the DPIA under review and ensure that it is updated if there are any changes (to the nature of the processing and/or system changes)

18. Signatories

The DPIA accurately reflects the processing and the residual risks have been approved by the Information Asset Owner:

Information Asset Owner (IAO) Signature and Date

Name	Role	Date
[redacted]	Information Asset Administrator (IAA)[37]	22/09/2026

[37] On behalf of the Information Asset Owner (IAO)

FOR OFFICE OF THE SIRO AND OFFICE OF THE DPO USE ONLY

19. Summary of high residual risks

Risk no.	High residual risk summary
1	**Technical measures:** There is a risk that insufficient technical controls are in place to ensure the security and integrity of NHS App data. Controls in place are deemed adequate based on current assessment but must be maintained via BAU
2	**Organisational measures:** There is a risk that organisational measures (e.g. training, governance, supplier oversight) are insufficient to safeguard NHS App data. Controls in place are deemed adequate based on current assessment but must be maintained via BAU.
9	**Third-party data processing/storage location:** There is a risk that NHS App data is being processed outside of NHS England's data processing risk appetite. Recommended actions for mitigation in progress.
20	**Lack of interstitial screens for linked services:** There is a risk that users will not understand that they have left the NHS App environment and may misattribute responsibility for the linked service, or may interact with services that do not meet NHS England's security or authentication standards. Recommended actions for mitigation in progress.

Summary of DPO advice:

Data Protection Officer (DPO) **Signature and Date**

ICO consultation outcome:

Office of DPO **Signature and Date**

Next Steps:

DPO to inform stakeholders of ICO consultation outcome

IAO along with DPO and SIRO to build action plan to align the processing to ICO's decision

Annex A – NHS App features – further details

Core NHS App	
Functionality[38]	Description of what users can do
Contact Details	• View their NHS number on the logged-in home page • View their Name on the logged-in home page • View their date of birth on the logged-in home page
Medical Records	• View their GP Summary Care Record • View their GP Detailed Coded Record • Download documents related to the GP health record
Prescriptions	• Order a repeat prescription • View their prescription order history (Requested medicines) • View their approved repeat prescriptions
Appointments	• Book a GP appointment • View their upcoming GP appointments • View their historical (past) GP appointments • Cancel a GP appointment
Set user research preferences	• Sign up for user research
Notifications	• Opt in and out of receiving NHS App push notifications[39]. • Receive NHS App push notifications and in-app messages[40]
Access in-app messages	• View messages from their GP surgery • Send their GP surgery a message • View attachments

[38] Viewing health records, making online consultation, ordering and managing medication, appointments, nominated pharmacy may depend on the user's GP practice.
[39] Users can choose their preferences for receiving updates and notifications from the NHS App. Users can opt out of push notifications at any time as they will be able to control this within their own device settings. In-App Messaging will be accessible to the user whilst they are using the NHS App.
[40] Available for both 3rd parties and the NHS App sending on behalf of

Core NHS App	
Functionality[38]	Description of what users can do
Manage their nominated pharmacy	• View their pharmacy nomination • Update their pharmacy nomination
Access third party integration connect to other services providing health and social care[41]	Access links to other health services, including mental health support or social care for: • Personal Health Records • Online Consultations • National Services • Notifications and Messaging (Primary and Secondary Care) • NHS Notify • Patient Care Aggregator (Wayfinder)
GP Proxy – Linked Profiles[42]	• View their linked profiles (Proxy profiles) • Carry out actions on behalf of others[43] (GP appointment booking, repeat prescriptions and health records only)
Biometric login (Native only)	• Enable iOS Touch & Face ID • Enable Android fingerprint login • Register and unregister
Cookies	• Allow optional analytic cookies
NHS Login Account Settings[44]	• View their NHS Login account settings • Change their NHS Login account password or email address • Delete their NHS Login account
Integrated Calendar (Native only)	• Add GP appointments to their device's calendar • Add reminders to request repeat prescriptions

[41] Connection to health and social care services depends on local service availability and their integration with the NHS App
[42] Enabling proxy access requires authorisation and setup by the user's GP practice
[43] See: https://digital.nhs.uk/developer/api-catalogue/nhs-app Different use cases support either sending by ODS code (broadcast, internal use) or targeted by NHS number (external use)
[44] Options may vary depending on P5 or P9

Core NHS App	
Functionality[38]	Description of what users can do
Relies on national integrations	
Vaccinations	• View their vaccination history • Access their COVID-19 vaccination records/certificates.
Organ donation	• View their organ donation preferences • Change their organ donation preferences
Get health advice	Users can access NHS-verified information about conditions, treatments and healthy living.
Data sharing preferences (National data opt out[45])	• View their data sharing preferences • Change their data sharing preferences
Support via NHS 111	• Check their symptoms • Get health advice
Other	
Desktop App	The NHS App is accessible via a web browser, offering the same features as the mobile app.
"Password-less" authentication:	The NHS App uses NHS login for its Authentication and Identity Assurance. Where the NHS App performs "Password-less" authentication against NHS login, this is done in accordance with the Fast Identity Online (FIDO) standard. Registered users of the NHS App can use the "Password-less" authentication feature if their mobile phone supports this. NHS login allows Passkeys to be used in the browser, so a user can login to the NHS App using a passkey if they are using a browser instead of the mobile app.

- Log & Analytical data – for reporting and error correction. User events and error data is collected from the NHS App during run-time and processed into a Data Platform (for Analytical purposes) and Splunk for (error investigation). The Analytical data is processed within the platform and all user event records are collated into aggregated data (without personal information) for reporting purposes within the NHS.
- Within Splunk, the events contain minimal User information (NHS Number & NHS Login ID) to allow for the investigation of errors within the usage

[45] See https://digital.nhs.uk/services/national-data-opt-out

Annex B – NHS App Notification and Messaging Services - Controller Table

Send and View Messages		
Actor / Entity	Data Role	Description
Sending Service e.g. GP practices	Controller (in respect of determining who to message, content of messages, when and how to communicate)	The sending service will curate all messages and send them to NHS App Messaging and is accountable for: • Who to message • Ensuring they only message individuals who they have a legal basis to send communications to • Ensuring a person's right to opt-out of communication is respected when to message • NHS App Messaging will deliver the message as soon as it is received, so it is the responsibility of the Sending Service to determine when someone should get the message how to message • Ensuring that NHS App Messaging is an appropriate communication channel for the individual being messaged what to message • Ensuring that the message content is accurate, well written and fit for purpose • Ensuring that the message is related to the individual's direct care
Communication Supplier	Processor	Appointed by the Sending Service, a 3rd party Communication Supplier could: • Facilitate the curation of the message • Including identification of individual's NHS Number • Message content • Have the integration with NHS App Messaging to process the sending of messages
NHS App Messaging and NHS App Notification	Joint Controller with Secretary of State for the delivery of the message through the NHS App	App Messaging and NHS App Notification Services will accept messages from verified Sending Service and Communication Suppliers, and deliver that message to the intended individual, which includes: • Access Control for the integrated part • Validation of Sender Identity

Services (NHS England)		• Validation of recipient NHS Number • Persistence of message in line with data retention policy • Notifying the recipient to the new message • Enabling the recipient to view the message • Responding to requests from the Citizen / Patient / NHS App user to manage aspects of the messages inbox • Replying to messages
Citizen / Patient / NHS App User	Data subject	The Citizen / Patient / NHS App User will be able to view their messages via the NHS App.
Check User Details[46]		
Actor / Entity	Data Role	Description
Sending Service & Communication Supplier	Controller Processor	The Sending Service or the Communication Supplier, automatically on the Sending Service's behalf, can use information about a user's registration and notification opt-in status to determine if NHS App Messaging is the most appropriate communication channel for an upcoming message. The information must only be used for this purpose.
NHS App Messaging and NHS App Notification Services (NHS England)	Joint Controller with Secretary of State for the delivery of the message through the NHS App	The NHS App Messaging and Push Notification Services will maintain a record of which NHS Numbers have registered for the NHS App and if they have opted in to notifications. This information is periodically refreshed to provide Sending Services / Communication Suppliers with up-to-date data in order to make a decision on to send or not.
Citizen / Patient / NHS App User	Data subject	When the user registers for the NHS App or configures their Notification preferences, this information triggers the process to update the User Details report.

[46] The user details information can be used by client applications to determine whether it is appropriate to attempt to use the NHS App Messaging, or if alternative communication channels should be used instead.

Check Message Status[47]		
Actor / Entity	Data Role	Description
Sending Service & Communication Supplier	Controller Processor	The Sending Service or the Communication Supplier, automatically on the Sending Service's behalf, can use information about a message's delivery status to: Ensure their communication methods are being effective Keep a record of communication attempts and the success of them The information must only be used for this purpose.
NHS App Messaging and NHS App Notification Services (NHS England)	Joint Controller with Secretary of State for the delivery of the message through the NHS App	The NHS App Messaging and NHS App Notification Services will maintain a record of if a message is: Received with success Received with failure Read by the Citizen / Patient / NHS App User
Citizen / Patient / NHS App User	Data subject	A record is kept when a message is successfully added to a user's inbox and when the user opens that message in the app.

[47] In order for Sending Services to fulfil their duty of care and keep a record of the communications they sent, the NHS App Messaging service provides a way to monitor the delivery status of a message.

Annex C – NHS App third-party products and integrations

Back-end suppliers, products and functionality	
Name	Product and/or functionality provided
Akamai	Kona Site Defender (Firewall) as part of DDoS and other cyber security protection, a redirect service, all routing for NHS UK, NHS App and 111 and the caching of web pages across all these channels.
Dig Inclusion	Annual accessibility audit.
Dionach	Annual PEN test.
Dragon	Speech recognition software for both front end and back-end applications
EMIS	Provides a test for NHS App which is used to ensure the continued delivery of the roadmap developed by NHS England for enhancements to the App functionality.
Figma	Industry-standard interface design tool used by all product teams in NHS England to design, prototype, and specify digital services.
Frutiger (Monotype)	Corporate font, which is contemporary and flexible sans serif font, which was designed to be clear and easy to read at a distance and in small size.
IBM	NHS England delivery partner for developing, running and maintaining the NHS App
Jetbrains	Integrated development environment tool used for developing code, particularly for iPhones.
Microsoft Azure	Cloud-based platform and the main hosting side of NHS App data.
NHS Federated Data Platform (FDP)	The NHS FDP will host the NHS App Analytics data (once the migration from Azure Databricks is complete)
Optimal Workshop	Tests NHS App information architecture and usability, identify issues and improve the user experience
Outcold Solutions (LLC Kubernetes)	Integration tool that integrates Kubernetes with Splunk to monitor the NHS App to ensure it is running reliable, robust and allow us to support incidents.
Phoenix Software	Adobe Analytics: Product used to provide insights into customer journeys, product engagement and usage and content performance

	Browserstack: Cloud web and mobile testing platform that provides developers with the ability to test their websites and mobile applications across on-demand browsers.
Pingdom	Monitors the latency of NHS App.
Qualtrics	Creates surveys and feedback polls, using a variety of distribution means.
Slack	Main communication tool used by NHS England and third-party contractors developing, running and maintaining the app
SPLUNK (Softcat PLC)	Application that monitors the health of national live services, detecting incidents, and alerting to suspicious activities
Teleperformance	Provides agents to triage tickets
Valiantis (Atlassian)	Jira/Confuence and all plugins used by NHS England and third-party contractors developing, running and maintaining the app for issue and bug tracking. Confluence used to share project updates and meeting updates
ZenDesk	Tool for managing citizen enquiries by a 3rd party first line support supplier Teleperformance, relating to the NHS App, NHS login or NHS Wayfinder services.
ZoomText Fusion	Fully integrated magnification and reading programme tailored for low vision users

Front-end suppliers, integrations/products and functionality With reference to Common Front-end Integration and Functionality definitions			
Organisation	Type	Product	Functionality
Accurx	Direct	Patient Triage	Medical query; Admin query (a, b, c, d)
	N&M (1)	N/A	Notifications and Messaging (1); Receipts
Capri Healthcare	Direct	V-Consult	Medical query; Admin query (c, e, f)
Cisco	PCA (2)	Healthcare Communications	Appointments (2); Documents (2); Paperless preference
Dr Doctor	N&M (2)	N/A	Notifications and Messaging (2); Receipts
	PCA (2)	DrDoctor	Appointments (2)
eConsult Health Limited	Direct	Web-GP	Medical query; Admin query (a, b, c, d)
East Kent Hospitals University Foundation Trust	PCA (2)	Path EKS2	Appointments (2+)
Engage Health Systems	Direct	Engage Consult	Medical query; Admin query (c, d)
Healthcall	N&M (2)	N/A	Notifications and Messaging (2); Receipts
	PCA (2)	My Health Call PEP	Appointments (2); Paperless preference; Documents (2); Questionnaires (2)
Induction Healthcare	N&M (2)	N/A	Notifications and Messaging (2); Receipts
	PCA (2)	Zesty	Appointments (2); Paperless preference; Documents (2); Questionnaires (2)
iPlato	Direct	MyGPTriage	Medical query; Admin query (a, b, c, d)
iPLATO Healthcare	N&M (1)	N/A	Notifications and Messaging (1); Receipts
Mediwave	PCA (2)	MAIA	Appointments (2+)
MJOG	N&M (1)	N/A	Notifications and Messaging (1); Receipts

Front-end suppliers, integrations/products and functionality With reference to Common Front-end Integration and Functionality definitions			
Organisation	Type	Product	Functionality
National Institute of Health Research	National	Be Part of Research	Sign-up for email updates about health and care research participation
Netcall	N&M (2)	N/A	Notifications and Messaging (2); Receipts
	PCA (2)	PatientHub	Appointments (2); Documents (2); Questionnaires (2); **MIv2:** Supports generation of management information
NHS England	National	Online GP Registration	Confirmation of registration at a new GP practice in England
	National	111 Online	Check your symptoms
	National	NBS[48]	Group booking
	National	Proxy Application Service	Offers patients the ability to request (or nominate) a proxy to act on their behalf in health and care
Patch's Health	Direct	Patchs	Medical query; Admin query (a, b, c, d, g, h)
Patients Know Best	Direct	PKB	Medical query
	PHR	PKB	• **Messaging:** Send and receive messages to and from your health and care professionals • **Library:** Access the library of shared links from providers • **Appointments:** View of provider appointments, with the ability to amend and cancel • **Care Plans:** Access to shared care planning, including collaborative care plans with the ability for all parties involved to access and update • **Health tracker:** Ability for patients to add entries to PKB health record under 'Symptoms', 'Measurements' (body & activity

[48] National Booking Service Spring Covid Campaign

Front-end suppliers, integrations/products and functionality With reference to Common Front-end Integration and Functionality definitions			
Organisation	Type	Product	Functionality
			including information from integrated apps and devices), and 'Journal' • **Medicines:** Access medicines prescribed by providers. Also provides the ability to record over-the-counter medicines • **Sharing:** Update your sharing preferences • **Documents:** Receive letters and other documents from your provider • **Test results and imaging:** Access results from a range of providers, including both the latest results and trends over time
	PCA (2)	PKB	Appointments (2)
	N&M (2)		Notifications and Messaging (2)
Universal Care Plan (UCP)	PHR	Better	**Care Plans:** Ask your GP about the information in your care plan
University Hospital Morecambe Bay NHS Foundation Trust	PCA (2)	PEP+	Appointments (2+)
University Hospital Southampton NHS Foundation Trust	PCA (2)	My Medical Record	Appointments (2)
Virtually	Direct	Virtually Healthcare	Medical query; Admin query (g, h, i)

NHS Notify Integrations[49]			
Organisation	Type	Product	Functionality being integrated
Accurx	Direct	Patient Triage	Medical query; Admin query (a, b, c, d)
	N&M (1)	N/A	Notifications and Messaging (1); Receipts
Capri Healthcare	Direct	V-Consult	Medical query; Admin query (c, e, f)
Cisco	PCA (2)	Healthcare Communications	Appointments (2); Documents (2); Paperless preference

[49] Since January 2024, NHS App Notification and Messaging integrations are being managed as part of the wider NHS Notify onboarding process.

Common Front-end Integration and Functionality definitions	
Integration	Definition
N&M (1/2)	Notification and messaging (Primary Care/Secondary Care)
PCA (2)	Patient Care Aggregator (Secondary Care Appointments)
PHR	Personal Health Records
Medical query	Ask your GP for medical advice
Admin query	Ask your GP for: (a) test results; (b) a doctor's letter; (c) a sick note; (d) referrals; (e) to change personal details; (f) update contact preferences You can also: (g) View past responses, (h) Check past requests, (i) send a new request
Notifications and Messaging (1)	Receive a notification and message from your GP
Notifications and Messaging (2)	Receive a notification and message about a secondary care appointment
Receipts	Notification has sent. Message read (Real time receipt)
Appointments (2)	You can view, amend or cancel secondary care appointments
Appointments (2+)	You can view, amend or cancel secondary care appointments. Access supporting appointment information. View single point of contact for appointment
Documents (2)	View documents related to secondary care appointments
Paperless preference	Select and manage paperless preference
Questionnaires (2)	View questionnaires related to secondary care appointments

Annex D – Subsidiary Risks transitioned to NHS App programme team registers:

Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk[50]	Residual risk[51]	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
Denial of service attack being launched against the NHS App **As a result of** the removal of geo-fencing, increasing its visibility to potential malicious actors. **There is a risk** that a person or organisation may launch a Denial of Service (DoS) attack against the NHS App, exploiting its expanded attack surface. **Which could result in:** 1. A disruption to the availability of the NHS App, including partial or complete service outages, which could then lead to 2. Reputational damage, reduced public trust, delayed access to care services (e.g. appointments, prescriptions), and clinical safety risks for patients reliant on timely digital access.	**High (12)**	**Existing Controls:** 1. The NHS App uses Akamai WAF and Site shield as their "front door" protection. The capability is set to trigger if a DoS attack is detected and block the incoming traffic from the detected IP Addresses. 2. Logs and configuration regularly reviewed with supplier 3. Rate-limiting and throttling are configured at the API Gateway to prevent excessive authenticated requests from	Treat	**Low (6)**	[redacted] Head of Delivery (NHS App) 22/01/2026	Controls in place are deemed adequate based on current assessment.

[50] Tolerate, Terminate, Treat or Transfer
[51] Low, Medium or High

Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk[50]	Residual risk[51]	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
Type of Risk: Operational (tech security)		degrading performance; alerting is in place for abnormal usage patterns.				
<u>Contaminated data via a compromised third-party service provider</u> **As a result of** one of the NHS App's third-party suppliers becoming compromised through an attack or a data breach (the NHS App uses over 30 front and back-end supplier to support functions and features). **There is a risk** that malicious or malformed data is transmitted from a compromised supplier to the NHS App via established API connections. **Which could result in:** 1. A data security breach or service contamination affecting NHS App performance or integrity, which could then lead to 2. Reputational damage, user disruption, regulatory scrutiny, and	**Moderate (9)**	**Existing Controls:** 1. The NHS App only receives plain text responses from the suppliers therefore no files or special characters are accepted by the APIs. 2. All APIs have been penetration tested before going live. 3. **Suppliers Conformance Assessment List (SCAL)** required confirming the supplier's adherence to security, compliance and technical standards.	Treat	**Low (6)**	[redacted] Head of Delivery (NHS App) 22/01/2026	Controls in place are deemed adequate based on current assessment.

Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk[50]	Residual risk[51]	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
downstream vulnerabilities in NHS England's digital supply chain. **Type of Risk:** Operational (tech security)		4. Suppliers processing data must demonstrate a commitment to the **Data Security Protection Toolkit**				
<u>Incorrectly matched or confused records</u> **As a result of** one or more of the following: 1. PDS incorrectly matching records; or 2. Failure in the NHS Login ID verification process; or 3. Incorrect matching carried out by primary or secondary healthcare services **There is a risk** that a user is matched to a record which isn't theirs (incorrect matching) or being shown data on a record which isn't theirs (confused records). **Which could result in:** 1. Disclosure of health information to an incorrect patient and a data breach. 2. This can cause distress and inconvenience, particularly if it results in the inability to access services through the NHS App until it	**Low (6)**	**Existing Controls:** 1. This risk is owned by the NHS Login programme, which keeps a detailed record of it. A copy is of the full risk as at 31/03/25 is available at Annex F. NHS Login will implement the appropriate verification and security controls, subject to prioritisation, to mitigate their risk. 2. NHS App continues to monitor via NHS Login updates and governance process.	Tolerate	**Low (6)**	[redacted] Head of Delivery (NHS App) 22/01/2026	This risk is owned by the NHS Login programme

Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk[50]	Residual risk[51]	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
is addressed. This in turn leads to compensation claims from affected individuals. **Type of Risk:** Legal, compliance and regulatory						
<u>App Messaging failures</u> **As a result of** technical failures, system outages or integration issues **There is a risk** that messages sent through the NHS App are not delivered to patients in a timely or accurate manner. **Which may result in:** 1. Disruption to patient communications, such as missed appointment reminders or care instructions, which could then lead to 2. Patient confusion or distress, complaints to NHS organisations, erosion of trust in the NHS App, and potential risks to care outcomes in borderline or vulnerable cases. 3. If the error includes potential breaches of UK GDPR principles of accuracy and integrity this could also lead to regulatory non-compliance.	**Moderate (9)**	**Existing controls** 1. The NHS App Messaging Service tracks the delivery status of messages and Sending Organisations and Communication Suppliers can use this information to act on those not delivered, and make the decision to communicate with the patient via other means e.g. fallback options such as SMS / email / telephone, etc. 2. The NHS App notification settings have been simplified	Treat	**Low (6)**	[redacted] Head of Delivery (NHS App) 22/01/2026	Controls in place are deemed adequate based on current assessment.

Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk[50]	Residual risk[51]	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
Type of Risk: Legal, compliance and regulatory Patient safety and quality of care		and are controlled at a device level, including enabling users to manage their push notification settings. 3. Healthcare providers under their duty of care to patients should be utilising follow-up protocols for contacting a patient where a message is deemed important enough that contact needs to be made with the patient, as it is expected that not all patients can or will use digital products.				
<u>Multiple User Accounts</u> **As a result of** an individual having multiple NHS login accounts verified at P9 level and mapped to the same NHS number **There is a risk** system-generated messages or notifications are sent to a	**Low (6)**	**Existing Controls:** 1. Since February 2023, it has not been possible for users to have more than one account that is verified at P9 level. Therefore, this risk	Tolerate	**Low (3)**	[redacted] Head of Delivery (NHS App) 22/01/2026	This risk is owned by the NHS Login programme.

Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk[50]	Residual risk[51]	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
dormant or inactive account instead of the one the individual actually uses **Which may result in:** 1. Important communications not being received, resulting in missed care interventions, increased risk to patient safety. 2. There is also the possibility of non-compliance with data protection principles around accuracy and integrity. These immediate impacts will incur reputational damage and erode patient trust. **Type of Risk:** Patient safety and quality of care Legal, compliance and regulatory		could only arise for users who created multiple accounts before this control was implemented, significantly mitigating the level of risk. 2. NHS App continues to monitor via NHS Login updates and governance process.				
<u>Accuracy of information provided by connected services</u> **As a result of** the NHS App displaying data (e.g. prescriptions, appointments, test results) pulled from connected services, which may provide inaccurate or outdated information.	**High (12)**	**Existing Controls** 1. The NHS App privacy notice advises users that they can report data integrity issues via the NHS App. NHS England maintains a service desk function which allows the user	Tolerate	**Moderate (8)**	[redacted] Head of Delivery (NHS App) 22/01/2026	Controls in place are deemed adequate based on current assessment. Further reduction would require control over connected

Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk[50]	Residual risk[51]	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
There is a risk that the NHS App displays information from a connected service that is not up-to-date or accurate. **Which may result in:** 1. Users relying on incorrect data to make decisions about their care, which could then lead to 2. Patient confusion or harm, complaints to NHS England or the connected service, increased service desk burden, potential breach of data protection principles (accuracy, accountability), reputational damage, and loss of public trust. If harm occurs, this may also lead to legal claims. 3. If the error includes potential breaches of UK GDPR principles of accuracy and integrity this could also lead to regulatory non-compliance. **Type of Risk:** Patient safety and quality of care Legal, compliance and regulatory		to interact with NHS England or the connected service to report the data integrity issues for resolution. 2. The NHS App utilises interstitial screens to advise the user when they are leaving the NHS App service, and moving onto a different service 3. NHS App users must agree to the Terms of Use, which includes provision on NHS England's liabilities to users (s10) relating to accuracy or how up-to-date information is that is being provided though services accessed through the app.				services' data quality, which is not currently within scope.

Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk[50]	Residual risk[51]	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
<u>Secondary use of data</u> **As a result of** secondary uses of NHS App data (e.g. for research, service evaluation, or improvement) not being clearly explained to users or drifting from the original healthcare delivery purpose. **There is a risk** that the NHS App is perceived to be processing personal data in a manner that is incompatible with the original purpose for which it was collected. **Which may lead to** 1. Users becoming uncomfortable or withdrawing from the NHS App due to lack of clarity or perceived misuse of data, which could then lead to 2. Legal challenges relating to data transparency, reduction in app uptake or trust, reputational damage, and scrutiny over NHS England's data governance practices. **Type of Risk:** Legal, compliance and regulatory	**Moderate (9)**	**Existing controls** 1. NHS App Privacy notice provides the user with a clear description of the processing. 2. Any Management Information requested will be subject to IG review and approval. 3. Where data requires a unique identifier, this will be the NHS login identifier which is classed as pseudonymised and can only meaningfully be associated with patient identifiable data once referenced within the NHS login system. 4. Any secondary use of data and linking will be subject to a DPIA for	Tolerate	**Low (6)**	[redacted] Head of Delivery (NHS App) 22/01/2026	Controls in place are deemed adequate based on current assessment.

Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk[50]	Residual risk[51]	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
		this activity and be reviewed by IG. 5. Any dissemination of data will be subject to review from the Advisory Group for Data.				
<u>Aggregated NHS App data on the NHS FDP</u> **As a result of** Aggregated NHS App analytics data ingested into the NHS Federated Data Platform including small numbers that are not suppressed, such as low-activity patterns or rare events. **There is a risk that** an individual could be re-identified (or inferred) from these small-number aggregates, if viewed in isolation or in combination with other data. **Which could result in:** 1. Anonymised data being classed as personal under UK GDPR due to residual identifiability, which could then lead to	**Moderate (9)**	**Existing controls** Aggregated Data ingested into the Product and/or made available via the NHS App analytics dashboard has small numbers included, a risk assessment was undertaken to ascertain if the Data continue to be Personal Data. Whilst small numbers are included/shown, they have been further aggregated at daily/weekly/monthly and therefore it would not be possible to re-identify an individual in the Data or for the output to be linked	Tolerate	**Low (6)**	[redacted] Head of Delivery (NHS App) 22/01/2026	Controls in place are deemed adequate based on current assessment.

Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk[50]	Residual risk[51]	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
2. Regulatory non-compliance, ICO scrutiny, reputational harm, internal audit findings, and questions about the privacy maturity of the NHS App analytics programme. **Type of risk:** Legal, compliance and regulatory		with other Data which would enable re-identification to the users of the dashboard. The Data is therefore considered to be appropriately aggregated and anonymous.				

Annex E - 2 Year past appointment retention – Now Closed

Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk[52]	Residual risk[53]	Measure approved (Name and Date)	Actions integrated back into project plan (Date and responsibility for completion)
<u>MVP Past Appointment Record Retention review</u> There is a risk that applying previously considered 8-year record retention for MVP past appointments was excessive and not in keeping with good records management principles, and other data protection principles (e.g., data minimisation) **As a result of** adopting an eight-year retention period for MVP past appointment data **There is a risk** that this retention period may be excessive and inconsistent with data minimisation principles under UK GDPR **Which may lead to** regulatory non-compliance and an increased	Low[54]	**Existing Controls** NHS England has reviewed the record retention application in line with the programme needs and instead applies a **Two-year retention period**.	Treat	Low	[redacted] Head of Delivery (NHS App) 02 May 2025	Existing controls and operations are sufficient Fazila Dingmar

[52] Tolerate, Terminate, Treat or Transfer
[53] Low, Medium or High
[54] L: More Likely Than Not, I: Minimal Impact

risk of data breaches over time. These immediate impacts will incur reputational damage and erode patient trust. **Type of Risk:** Legal, compliance and regulatory						

Annex F – Glossary of terms (full descriptions)

Term	Definition
API	Application Programming Interface - Set of rules and protocols that allow software components to communicate and interact
BAU	Business As Usual - Regular operational activities carried out routinely within an organization
CCS	Crown Commercial Service - The UK government agency that provides commercial and procurement services for the public sector
CSP	Cloud Service Provider - Offers network services, infrastructure, or business applications in the cloud
DARS	Data Access Request Service - NHS service that manages requests for access to health and social care data
DHSC	Department of Health and Social Care - The UK government department responsible for public health and social care
DOS	Digital Outcomes and Specialists (procurement framework) - Procurement framework that enables public sector buyers to access digital expertise
DPIA	Data Protection Impact Assessment - Process to assess and mitigate privacy risks in data processing activities
DSPT	Data Security and Protection Toolkit - Self-assessment tool for NHS and care organisations to demonstrate data security compliance.
EPS	Electronic Prescription Service - NHS system that enables prescriptions to be sent electronically from GP to pharmacy.
FDP	Federated Data Platform - Shared infrastructure allowing secure, interoperable access to health and care data
FHIR	Fast Healthcare Interoperability Resources - Standard for exchanging healthcare information electronically
GPIT	General Practice IT - The systems, software, and digital infrastructure used in general practice settings
ICB	Integrated Care Board – Regionally distributed NHS bodies responsible for planning and funding local healthcare services
IM1	Interface Mechanism 1 - Standard API used to integrate third-party applications with NHS GP systems
NDC	National Digital Channels - Central NHS platforms (e.g., NHS App, NHS.uk) that provide digital health services
NDIT	National Data Ingestion Tenant - Centralised data collection point within NHS infrastructure for ingesting health data
NDOO	National Data Opt-Out - NHS policy allowing individuals to opt out of sharing their confidential data for research and planning
NHSA	National Health Service Act (Isle of Man) - Refers to the legislation that governs the NHS, including variants like the Isle of Man Act
NICE	National Institute for Health and Care Excellence - The UK body that provides guidance and recommendations on health and care practices
OLC	Online Consultation - Digital method for patients to contact their GP or healthcare provider without a face-to-face visit
ODS	Organisation Data Service - The NHS service that issues and maintains unique identifiers for organisations and professionals
PET	Privacy Enhancing Technology - Tools and approaches used to protect personal data and maintain privacy

PHR	Personal Health Record - Digital record maintained by the individual that contains their health information
PID	Personally Identifiable Data - Data that can be used to identify a specific individual (e.g., name, NHS number)
RDDT	Regional Director of Digital Transformation - Role overseeing digital transformation within NHS regional areas
SLSP	System Level Security Policy - Policy that defines the security controls and responsibilities within a specific system
SME	Subject Matter Expert - Individual with deep expertise in a specific area, often consulted for their specialist knowledge
SMS	Short Message Service - Standard technology for sending text messages to mobile phones (text messaging)
Spine	The central NHS digital infrastructure that supports key services such as electronic prescriptions and patient demographics
UK GDPR	United Kingdom General Data Protection Regulation - UK law governing the use and protection of personal data
WAF	Web Application Firewall - Security system that protects web applications by filtering and monitoring HTTP traffic
Wayfinder	NHS system for aggregating and presenting referral data from secondary care and presents it to clinicians to support patient care decisions
e-RS	e-Referral Service - The NHS digital service used to manage and book patient referrals to specialist services