

Document filename:	Annex B - Requirements Specification for NHS login Services		
Project / Programme	NHS login		
Document Reference			
Project Manager	[REDACTED]	Status	Final
Owner	[REDACTED]	Version	1.0
Author	[REDACTED]	Version issue date	05/08/2024

NHS login Services - Requirements Specification

Document management

Revision History

Version	Date	Summary of Changes
0.1	26/05/2020	Uplifted to the new template
0.2	27/05/2020	Reviewed and revised by IG
0.3	27/05/2020	Uplifted to reflect IG comments
0.4	27/05/2020	Dissemination section regarding devolved admins edited
0.5	14/06/2020	Updated to reflect comments from review of 0.4 – Devolved Nations
0.6	16/07/2020	Updated following review of the directions by DHSC and NHSD Legal
0.7	31/07/2020	Updated following feedback from the Programme, NHSX and NHSD Legal
0.8	27/08/2020	Comments and amendments accepted
0.9	25/08/2021	Review and update to reflect the use of NHS login outside of England
1.0	30/01/2024	Review and update to reflect NHS login services, organisational changes and data analytics use.
1.0	5/8/2024	Taken to final and published

Reviewers

This document must be reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version
[REDACTED]	NHS login IG Lead	30/01/2024	1.0
[REDACTED]	IG Lead	27/06/2024	1.0

Approved by

This document must be approved by the following people:

Name	Title	Date	Version
[REDACTED]	NHS login IAO	27/06/2024	1.0

Glossary of Terms

Term / Abbreviation	What it stands for
PIB	NHS login Partner Integration Board
Proxy	Proxy access is where a trusted person, called a "proxy", can act on behalf of a patient to support them in their care. This can include access to a patient's medical record, but also covers the proxy's use of transactional services, like appointments or repeat prescriptions.
GPITF	GP IT Futures

Document Control:

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

Purpose of document

This document sets out the requirements for the NHS login Services and should be read alongside the:

- [NHS login Directions 2021](#) issued by the Secretary of State for Health and Social Care, which replaced the “Health and Social Care Information Centre (Establishment of Information Systems for NHS Services: Citizen Identity Services) Directions 2018” issued by NHS England, which was revoked by NHS England; and
- Annex A - Citizen Identity (NHS login) Technical Definition

Introduction

NHS England has been directed by the Secretary of State to support the provision of secure identity verification and authentication for digital services, (collectively, the **NHS login Services**), assessed by the Partner Integration Board¹ (**PIB**) as being beneficial to health services and adult social care services in England; and to the recipients of health and adult social care services provided in England.

Purpose of the NHS login Services

The data processed by the NHS login Services will be used to support the following scenarios:

- Providing access to digital health and social care services which have been commissioned by the NHS in England and have been approved by the PIB;
- Providing access to other digital health and social care services where the services are considered to be in the interests of the health service in England or the recipients or providers of adult social care in England;²
- Providing access to digital health and social care services which have been commissioned within Wales and have been approved by the PIB.
- Delivery of an NHS login ID verification and authentication service which can be used as a ‘federated’ capability to provide access across multiple digital services within England;
- Providing NHS login ID verification and authentication service to digital services which have been approved for use on behalf of countries outside of England;
- Providing personal data about NHS login users to health and care professionals for direct care purposes;
- Supporting commissioners and policy teams by providing statistical data to achieve positive health outcomes;
- Providing data about NHS login users to NHS England data and management information services for the purpose of improving user experience, to determine future

¹ The NHS login Partner Integration Board (PIB) is a standing committee accountable to the NHS login Product Board. The PIB reviews and approves any activity related to third parties connecting to NHS login.

² Applications will be considered by the DHSC and NHS England, dependent on the policy area concerned. Such considerations will also take into account any recommendations of the Partner Integration Board.

digital investments and strategy and to support internal and external reporting on the use of NHS England services, such as the NHS website and NHS App;

- Supporting those digital services that are assessed as beneficial to the health services, to social care services and to the recipients of health and adult social care services in England;

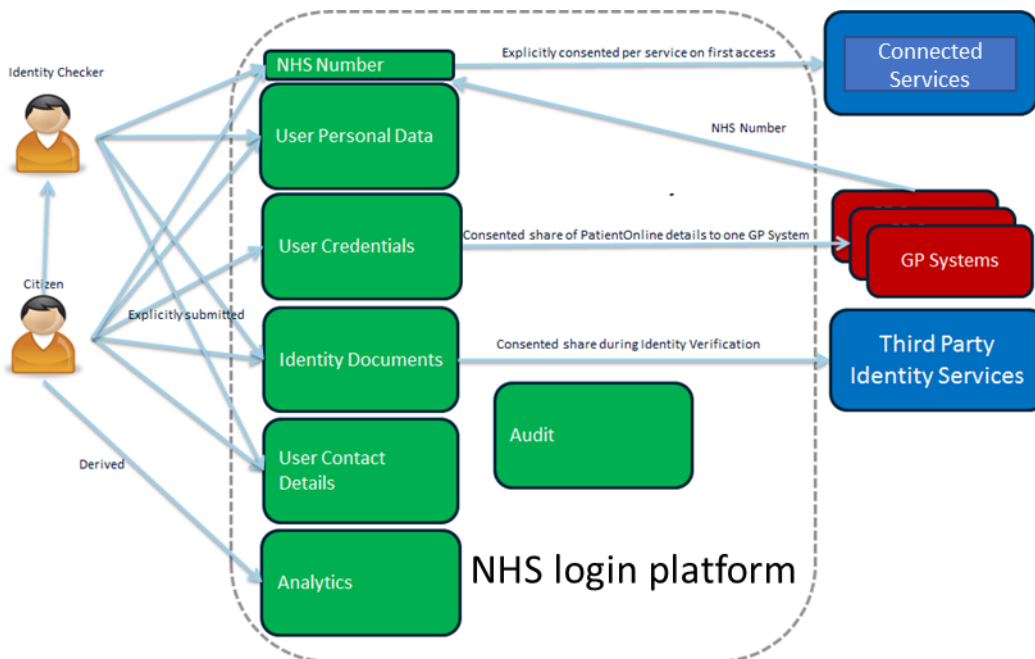
Supporting users

In providing the NHS login Services, NHS England will:

- Ensure that users can manage their NHS login account and control how their data is used to support Connected services;
- Invite users to participate in user research so that the NHS login Services can be developed and enhanced;
- Provide a single NHS login account, so that users can access other Connected services which use NHS login.

An overview of the service is illustrated below and supported by the following definitions:

- Connected Services – A digital service which utilises NHS login that meets the Partner Integration Board criteria and is Onboarded in line with the Assurance and Governance requirements set out within NHS England’s Connection Agreement;
- GP Systems – As defined within GP IT Futures (GPITF);
- Third Party Identity Services – As contracted by NHS login to deliver an ID Verification and Authentication service.



Data collection

Scope

The NHS login Services will use personal data provided by the data subject for the purposes of ID verification and Authentication. The data provided to NHS login may be shared with NHS England or a Digital Connected service if the data subject has agreed to this.

Source

Personal data processed by NHS Login Services will be provided:

- by the data subject, irrespective of the service used by the user
- by the Personal Demographic Service (PDS)
- by the National Proxy Service
- by GP Systems

Category

The personal data processed will comprise of the following:

Data Categories	Yes/No	Explanation
Personal Data		
Name	Yes	First names and surnames will be collected for all users so the user can be accurately matched to their record. This field is one of the 'mandatory fields' on which the Personal Demographic Service (PDS) look up is based in order to find an NHS record for a data subject. The middle name may be processed if it's included within the ID document or provided by the data subject.
Address	Yes	The address is processed during the ID document check if provided within documents such as a UK drivers licence.
Postcode	Yes	The postcode is collected as part of one of the verification journeys available to the data subject. This data set is needed to match against the postcode within the data subject's record.
DOB	Yes	DOB will be collected for all users, so the user can be accurately matched to their record.
Age	Yes	This can be derived from the form of evidence provided by the user/delegated individual.

Sex	Yes	This can be derived from the subset of information contained in the passport and when the user submits a photo/video selfie.
Gender	Yes	This can be derived from the subset of information contained in the passport and when the user submits a photo/video selfie.
Email Address	Yes	An email address will be used as a part of the authentication credentials the user has to access the NHS login service.
Physical Description	Yes	This is derived from the video selfie, driving licence and passport photos.
General Identifier e.g. NHS No	Yes	The NHS number will be utilised to match against the PDS data set to authenticate and match the individual to a record. NHS Number may also be sent to Connected Services which the data subject uses once explicit consent has been received from the data subject.
Mobile/Landline Phone Number	Yes	A code could be sent to the individual's mobile and or landline phone number for 2 Factor Authentication, as a security measure for their NHS Account. Where an individual's mobile and/or landline phone number has been authenticated, NHS login may use this phone number, alongside GP Online Credentials, to enable a match of the individual to a record.
Online Identifier e.g. IP Address/Event Logs	Yes	Audit/event logs will be generated and will contain IP addresses. These will be stored within the Platform Protective Monitoring function securely; these logs may be utilised for investigative and legal requests.
Website Cookies	Yes	These will be for non-essential and essential cookies. Data subjects are made aware of the cookies used as this is stated within our Cookie Policy.
Mobile Phone / Landline Phone/ Device No / IMEI No	Yes	This could be derived. The IMEI and IMSI numbers will not be directly requested but may be accessible by a determined threat actor who exploits the knowledge of the user's mobile phone number.
GP/Patient Online Credentials	Yes	GP Online Credentials may be utilised to verify and match the data subject to a record.

		GP Online Credentials may be entered by the data subject or retrieved by the NHS login service.
Authentication	Yes	For the purposes of multi-factor authentication, NHS login will process passwords and receive secure public keys through device based biometric or passkey authentication*. *Biometric and passkey data will not be processed directly by NHS login.
Proxy	Yes	The details of Proxy relationships and corresponding proxy subject details, including NHS Number(s), may be sent to Connected services, once explicit consent has been received from the data subject. Proxy relationships and associated access permissions will be established by the National Proxy Service.
Audit Data	Yes	Audit is essential to record events conducted on the system and service. This supports investigations, accountability, and access control to the NHS login service.
Analytics	Yes	Analytics provides data that can be used to measure the performance and success of the of the service and is used to improve performance and user experience. Cookies used for analytics are non-essential cookies - the data subject can opt out of non-essential cookies. This is made clear in the Cookie Policy.
Special Category Data		
Racial / Ethnic Origin	Yes	This may be derived from personal information provided from the selfie or identity document.
Biometric Data (Fingerprints / Facial Recognition)	Yes	NHS login conduct a Liveness and Likeness check of a data subject in line with the elements of the NHS ID and Verification Standard. This is done via: <ul style="list-style-type: none"> • a video selfie, with a comparison of the photo(s) within the driving licence and passport; • contracted supplier's facial recognition software to support a solution to support ID verification at scale.

Frequency

The data has been, and is being, collected by NHS login since the service went into Private Beta in September 2018. Collection will be ongoing under the NHS login Directions 2021 from the Secretary of State to support new users and services.

Analysis

Internal processing

- Validation and matching to data held by NHS England, such as PDS data. NHS login validates the submitted personal data against the data held by NHS England so that the user can be matched to a registered NHS number and/or record.
- NHS login will use tools such as Hotjar to allow a mechanism for users to, optionally, provide feedback so that service can be improved.
- NHS login will use tools such as Adobe Analytics to review the way a user accesses the service and understand pain points along the journey so that the service can be improved.
- User research to support the continued improvement of the service by inviting users to take part in interviews/usability tests and surveys.
- Provide data as part of the Corporate Protective Monitoring service managed and delivered by NHS England's Cyber Security Operations Centre.
Provide data and management information within NHS England, to support improvements to user experience, to determine future digital investments and strategy and to support reporting on the use of NHS England services, such as the NHS website and NHS App, such reporting would be limited to aggregated data that does not identify an individual.

Data linkage

To create an NHS login account, the NHS login Services link the user submitted data to an NHS number held by NHS England.

Consultation

The consultation process included:

- User consultation (citizens), clinical consultation and a "Discovery Sprint" with the Cabinet Office Verify team;
- NHS England Information Assurance and Cyber Security Committee (IACSC), which includes (but is not limited to) the CEO, Medical Director, Caldicott Guardian, Cyber Security and Information Assurance Office, was consulted on the NHS CIP Security Case and supported its findings. This initial consultation with IACSC formed the basis for the Identity Verification and Authentication Standard for Health and Care;
- Professional and government bodies on both the Identity Verification and Authentication Standard for Health and Care and the overall strategy of the NHS Login Service;

- Stakeholders consulted include NHS England, Government Digital Service (GDS), Care Quality Commission (CQC), British Medical Association (BMA), Royal College of GPs (RCGP), Joint GP IT Committee (JGPIT), Privacy Consumer Advisory Group (PCAG) and the Department of Health and Social Care;
- The Programme has also actively participated in several supplier focused events including TechUK;
- There will be ongoing user research to progress and develop the NHS login Services.

Dissemination/Sharing

Regular Dissemination/Sharing

NHS England may provide the following reporting, such reporting would be limited to aggregated data that does not identify an individual:

- **To support individual access to digital health and social care services.** To provide digital health and social care services with information about which other digital tools a person is using. For example, to be able to easily show within the NHS App which other NHS login enabled apps, such as PHRs or Long-term condition management apps a person is using, for the purposes of providing the ability to easily access those services.
- **For use by health and care professionals for direct care purposes.** For example, so that a Health Visitor can see whether a person is using a digital version of a personal child health record or DPCHR.
- **To support DHSC and NHS commissioners and policy teams.** Anonymous information on uptake of digital services will be used to support the provisions required in order to achieve positive health outcomes for the population and reduce inequalities in health, including obligations under the Equality Act 2010.
- **To support data analytics and reporting.** Anonymous outputs from NHS England data analysis may be shared externally. In all cases, where data is shared users must opt in.
- **Statistical information about service usage.** Anonymous information may be shared on a periodic and ad-hoc basis to:
 1. The Department of Health and Social Care and its associated bodies
 2. Connected Services
- **For Connected Services.** Where the user chooses to do so, personal information may be shared between NHS login Services and the Connected service in line with the consent model designed as part of the Service.

Data Access Request Service (DARS)

There will be no dissemination of data via DARS as the data collected will not be onboarded and will not be made available to DARS applicants.

Publication

Data to be published

Data collected as a result of NHS login will be used to compile statistical charts and dashboard information.

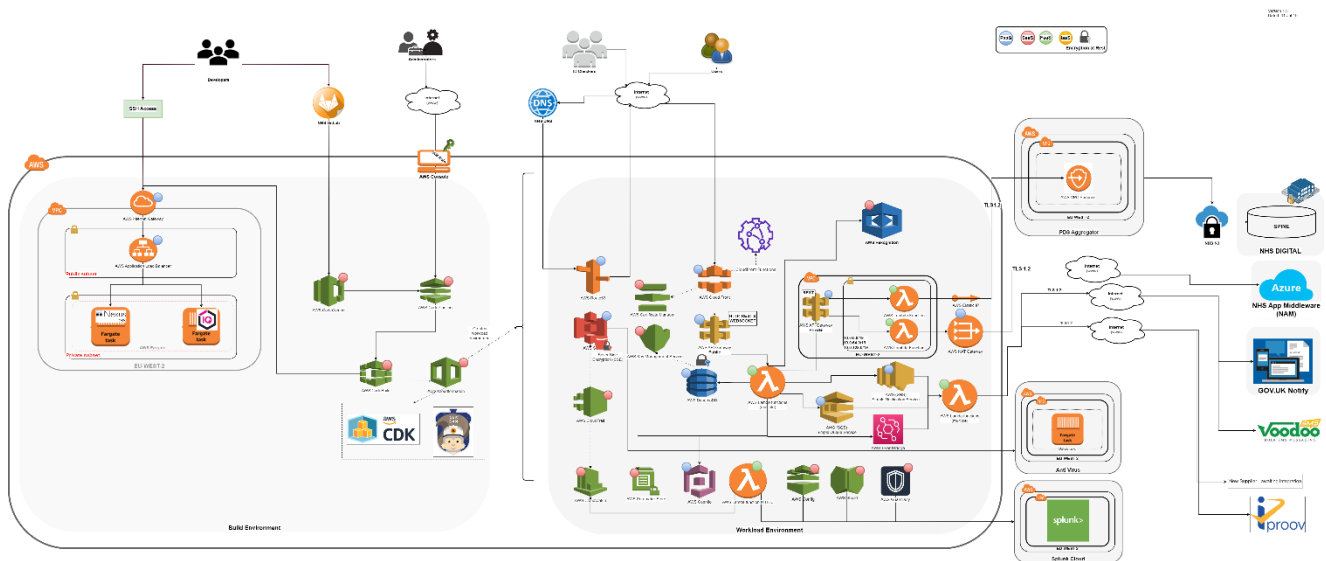
Data prohibited from being published

Information will be published in line with NHS England's duty to publish under section 260(1) of the Health and Social Care Act 2012, unless it falls within section 260(2) of the Act. For the avoidance of doubt the following data is specifically excluded from publication:

- Identifying or identifiable information about NHS login users

System Delivery Function

The diagram below provides an illustration of the service. Key components of the service are described below, and additional content is set out in the Technical Specification.



- **AWS.** NHS login is a cloud-based service hosted on Amazon Web Services (AWS).
- **SMS notification services.** NHS login use Gov. Notify, Voodoo and AWS SMS services as the mechanism to deliver the two-factor authentication codes.
- **ID verification services.** NHS login have established a team of trained manual ID checkers to deliver an ID verification service. The manual process is supported by ID supplier services which provide the programme with a scalable mechanism to deal with ID verification surge requests.
- **Re-use of GP/Patient Online credentials.** Where users have already verified their identity within a GP Practice and have been issued with GP/Patient Online credentials, NHS login can re-use these credentials to complete a match between an individual and an NHS record. Users can either enter the credentials or NHS login can check for the existence of GP/Patient Online Credentials and a corresponding match between authenticated contact details and NHS England held data to determine an NHS Number match.
- **Performance monitoring.** NHS login uses Splunk performance monitoring software to manage and monitor the platform.
- **User experience and feedback.** Hotjar A-B testing tool (VWO) and Qualtrics
- **Analytics.** Adobe Analytics and PowerBI.

Change control process

NHS England will manage any changes to this Specification in conjunction with, and by written agreement of an authorised officer of the Department of Health and Social Care.