Document filename:	**Requirements Specification for NHS Login**		
Project / Programme		Project NHS login	
Document Reference	**TBC**		
Project Manager		Status	**Draft**
Owner	Melissa Ruscoe	Version	**0.5**
Author	Brendon Plant	Version issue date	**14/06/2020**

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

Reviewers

This document must be reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version
Melissa Ruscoe	NHS login Programme Head	26/05/2020	0.5

Approved by

This document must be approved by the following people:

Name	Signature	Title	Date	Version
Melissa Ruscoe		Programme Head	26/05/2020	0.5

Glossary of Terms

Term / Abbreviation	What it stands for

Document Control:

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

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 will replace and revoke the “Health and Social Care Information Centre (Establishment of Information Systems for NHS Services: Citizen Identity Services) Directions 2018” issued by NHS England; and
- Citizen Identity (NHS login) Technical Definition (**the Technical Specification**).

Introduction

NHS Digital 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 as beneficial to health services; to social care services; and to the health of individuals.

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 NHS England or a Clinical Commissioning Group (CCG);
- Providing access to other digital health and social care services which have **not** been commissioned by NHS England or a CCG;
- Providing a secure ID verification and authentication service, using manual and automated tools for:
    - Local authorities;
    - Devolved agencies, where there is a separate legal authority to do so;
- 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;
- Provide personal data about NHS login users to health and care professionals for direct care purposes;
- To support commissioners and policy teams by providing statistical data to achieve positive health outcomes;
- To support those digital services that are assessed as beneficial to the NHS service, to social care services and to the recipients of health and care services provided in England

Supporting users

In providing the NHS Login Services, NHS Digital will:

- Ensure that users can manage their NHS login account and control how their data is used to support Connected services;

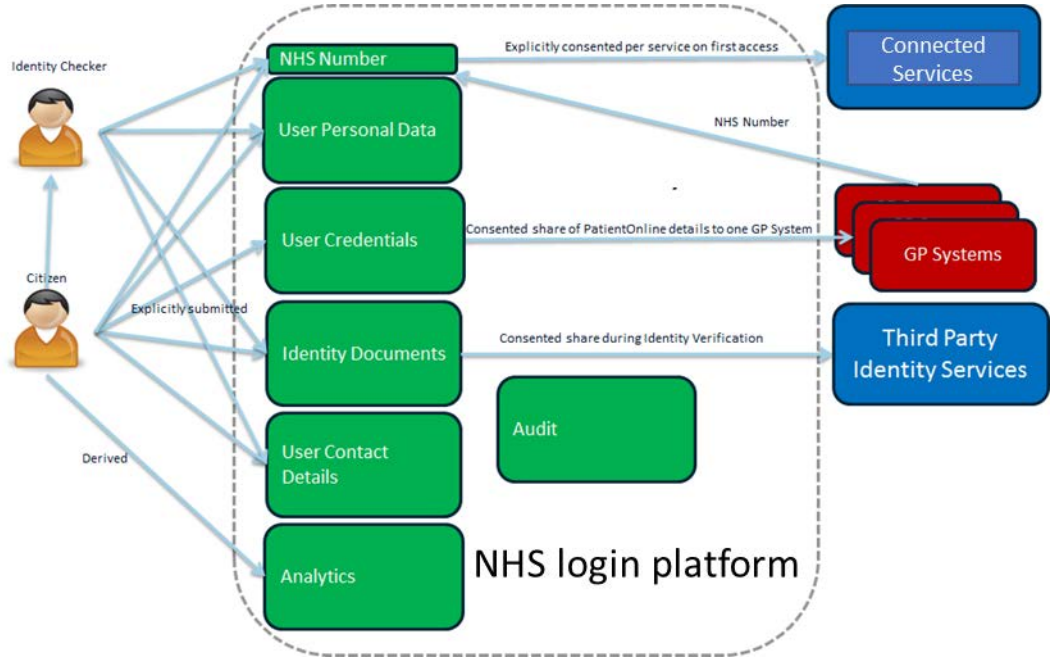
- Invite users to participate in user research so that the NHS Login Services can be developed and enhanced;
- Provide a coherent view to the user so that they can manage the way they access other Connected services which use the NHS Login Services.

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 Digital's Connection Agreement;

- GP Systems – As defined within GP Systems Of Choice (GPSOC) or 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 demographic data provided by the data subject for the purposes of ID verification and Authentication. The data provided to NHS login may be shared with 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).

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 we can accurately match them to their record. This field is one of the 'mandatory fields' with which we base our look up to PDS in order to find an NHS record for the data subject. The middle name may be processed if its 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 subjects record.
DOB	Yes	The DOB will be collected for all users, so we can accurately match them to their record.
Age	Yes	This can be derived from the form of evidence provided by patient/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	As per the statement for 'sex'.
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 NHS Personal Demographic Service (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 Phone Number	Yes	A code could be sent to the patient's mobile phone number for 2 Factor Authentication, as a security measure for their NHS Account.
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 / 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.
Audit Data	Yes	Audit is essential to record events conducted on our 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 - Data subject can opt out on the use of these. 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: - 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 in accordance with the NHS England Citizen ID Directions. 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 on PDS. NHS login validates the submitted personal data against the data held on PDS so that the user can be matched to a registered NHS number on PDS;
- 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 Digital's Cyber Security Operations Centre.

Data linkage

To create an NHS login account, the NHS Login Services link the user submitted data to an NHS number held on PDS.

Consultation

The consultation process included:

- User consultation (citizens), clinical consultation and a "Discovery Sprint" with the Cabinet Office Verify team;
- NHS Digital 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

- For use by the person/citizen. To provide other NHS provided services that the person is using with information about which other digital tools (that use NHS Login) that the 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 commissioners and policy teams. 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 our obligations under the Equality act.
- Statistical information about service usage – which will not contain personally identifiable information may be shared on a periodic and ad-hoc basis to:
    - The Department of Health and Social Care and its associated bodies, including but not limited to:
        - NHS England
        - NHSX
        - Public Health England
- 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

Publication

Data to be published

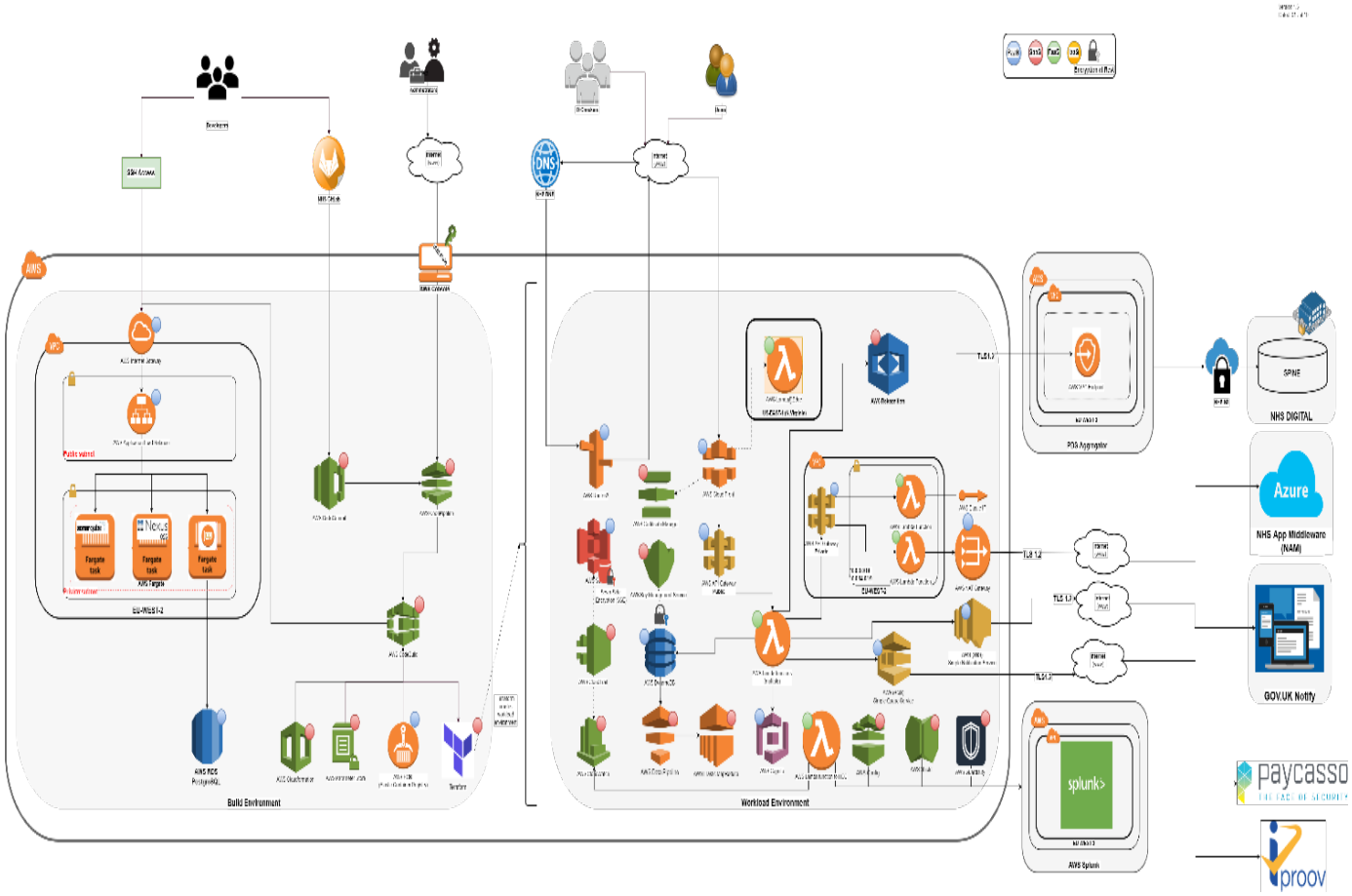
Data provided by NHS login users will be used to compile statistical charts and dashboard information in line with the dissemination and sharing statement.

Data prohibited from being published

TBC

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.
- Performance monitoring. NHS login use Splunk performance monitoring software to manage and monitor the platform.
- User experience and feedback – Hotjar.
- Analytics – Adobe Analytics.

Change control process

NHS Digital 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. Where necessary, NHS X and NHS England will be consulted on the changes.