Document filename:	**NHS login - Data Protection Impact Assessment (DPIA)**		
Directorate / Programme	**NHS login**		
Document Reference	**NHS login/DPIA**	[redacted]	
Information Asset Owner	[redacted]	Version	**2.7**
Author	[redacted]	Version issue date	**11/02/2026**

NHS login Data Protection Impact Assessment

Document Management

Revision History

Version	Date	Summary of Changes
0.1	Dec 2017	Incorporation of NHS login Programme comments
0.2	Feb 2018	Incorporation of NHS login Programme and IG Assurance comments
0.3	Feb 2018	Incorporation of NHS login Technical Lead comments
0.4	Mar 2018	Incorporation of IG Assurance comments
0.5	Apr 2018	Incorporation of NHS login Programme comments
1.0	May 2018	Final Version
1.1	10 Aug 2018	Reviewed an update in line with DLA Piper meeting
1.2	14 Aug 2018	Updated post Office of SIRO meeting with [redacted]
1.3	15 Aug 2018	Updated post review with Relying Party
1.4	20 Aug 2018	Updated post response from DLA Piper
1.5	31 Aug 2018	Updated prior to Management Review
1.6	13 Sep 2018	Management comments incorporated
1.7	03 Dec 2018	Updated to reflect PII usage in environment and review points since Sep 2018
1.8	26 Mar 2019	Updated formatting change CID to NHS Login; Right to Erasure/Deletion of Account; removed 10 yr account validity in line with passport date.
1.9	22 Jul 2019	Updated to reflect new template
1.10	18 Sep 2019	Updated following comments from IG
1.11	01 Oct 2019	Updated following comments from IG
1.12	01 Nov 2019	Review and updated to reflect suppliers Privacy Notice paragraph requirement and onboarding models
1.13	06 Nov 2019	Updated to reflect NHS App OLC use of NHS login processed data
1.14	01 Feb 2020	Updated to reflect eRS data flow transaction
1.15	27 Aug 2020	Reviewed by IG - comments and amendments added
1.16	15 Sep 2020	Transparency regarding the age control applied by partner services.
1.17	18 Nov 2020	Uplifted to address the use of NHS login outside of England.
1.18	03 Dec 2020	Uplifted to reflect use of services at P0; IoM; LHCRE
1.19	09 Dec 2020	Uplifted to reflect the use of NHS login with the Test and Trace Support Payment Scheme service
2.0	01 May 2021	Uplifted to reflect change of Legal Direction from NHS E to DHSC and to reference the use of the service by Covid-19 vaccination status and view my record services.
2.1	15 Jun 2021	Uplifted to reflect the use of NHS login by Covid Status services for users in Wales, A-B testing tools and R&D surveys
2.2	25 Aug 2021	Review pending s255 submission to EMT for the use of services by IoM DHSCC
2.3	23/10/2023	Updated to reflect merger and to include NHS Wales's use of NHS login
2.4-2.6	29/02/2024	Uplift to data items processed and consolidation of internal versions

2.7	11/02/2026	Uplift to new DPIA template, data items processed, risks and mitigations

Reviewers*

This document must be reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version
[redacted]	Cyber Security	26/02/2026	2.7
[redacted]	Information Governance	24/02/2026	2.7
[redacted]	Clinical Safety	26/02/2026	2.7

* NB: This table reflects the most recent version reviewed by an individual.

Approved by

This document must be approved by the following people:

Name	Title / Responsibility	Date	Version
[redacted]	NHS login IAO	11/02/2026	2.7

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.

Contents

1. Glossary of Terms

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

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
DPO	Data Protection Officer
DSPT	Data Security and Protection Toolkit
EPS	Electronic Prescription Service
FDP	Federated Data Platform
FHIR	Fast Healthcare Interoperability Resources
GPIT	General Practice IT
HMPO	His Majesty's Passport Office
IAO	Information Asset Owner
ICB	Integrated Care Board
ICO	Information Commissioner's Office
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
PDS	Personal Demographics Service
PET	Privacy Enhancing Technology
PHR	Personal Health Record
PID	Personally Identifiable Data
PRADO	Public Register of Authentic identity and travel Documents Online
PTT	Privacy, Transparency and Trust
RDDT	Regional Director of Digital Transformation
SIRO	Senior Information Risk Owner
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

2. 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.

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”. If you are unsure whether a DPIA is necessary, you should complete a DPIA screening questionnaire to assess whether the processing you are carrying out is regarded as high risk.

By completing a DPIA you can systematically analyse your processing to demonstrate how you will comply with data protection law and in doing so identify and minimise data protection risks.

This document should be read in conjunction with the DPIA Guidance and DPIA Screening Questionnaire

3. Introduction

Vision

The overarching vision of NHS login is to provide a secure, seamless, and user-friendly digital identity platform that enables individuals to access a wide range of health and adult social care services online, reducing avoidable demand on front line NHS and adult social care services, and facilitating a channel shift of patients and carers to digital services.

NHS login plays a pivotal role in delivering the NHS 10 Year Plan by enabling the digital transformation that underpins many of its core ambitions, this includes enabling digital access, supporting integrated care, empowering patients to have greater control, facilitating safe data sharing and providing a foundation for the innovation and development of future services.

Objectives

1. **Drive efficiencies to the NHS** and adult social care services – by providing information, tools and services to people digitally enabling people to self-serve, we will help to drive efficiencies.
2. **Improvements in People's Experience** – by bringing everything together for people regardless of where the service is commissioned, masking the complex structure of the NHS and adult social care services; making it easy to interact and transact digitally; giving people greater access to their information and providing transparency and clarity.
3. **Improve Health and Adult Social Care Outcomes** – by providing easier digital access, greater engagement through greater transparency, more information, tools, and services and better being able to target messages to people through their channel of choice, we will improve health outcomes and respond to the prevention agenda aspirations.

NHS login Key Performance Indicators

- Monthly successful user journey completions
- Level of identity verification risk
- Quality of end-to-end user experience
- NHS productivity savings
- NHS login operational costs

4. Consultation with Stakeholders

Stakeholder engagement has been built into the process for conducting the DPIA and associated review and refresh[1]. Key stakeholder types are outlined below:

Stakeholder type	Detail of engagement
Users	Integral and embedded engagement as part of service user research, user feedback, and support operations.
Commissioners	Proportionate and ongoing engagement as part of Product and Platforms wide governance and management.
Department of Health and Social Care (DHSC)	Proportionate and ongoing engagement as part of Product and Platforms wide governance and management.
Government Digital Services	Ongoing engagement through monthly engagement sessions and cross collaboration
Internal and External legal advisors	Proportionate and ongoing interface with internal legal advisors. External legal advisors engaged ad hoc for specialist advice.
Internal Stakeholders	Proportionate and ongoing interface with key internal stakeholders through NHS England's governance and account management for: • Information Governance • Commercial • Cyber Security • Clinical Safety
Care Quality Commission	Engagement at service and product initiation. Endorsed the Identity Verification and Authentication Standard for Health and Care Digital, Data, Analytics and Technology Use (DAPB3051).
British Medical Association	Engagement at service and product initiation. Endorsed DAPB3051.
Royal College of GPs	Engagement at service and product initiation. Endorsed DAPB3051.
Joint GP IT Committee	Engagement at service and product initiation. Endorsed DAPB3051.
Privacy Consumer Advisory (PCAG)	Engagement at service and product initiation. Endorsed DAPB3051.
The Information Assurance and Cyber Security	Engagement at service and product initiation. Endorsed DAPB3051.

[1] Consultation on further changes will occur where required and this section will be updated when consultation is done.

Stakeholder type	Detail of engagement
Committee (IACSC)	

NHS login has incorporated user consultation and engagement into its service delivery through several structured approaches, particularly aligned with NHS England's broader digital service standards and integration frameworks.

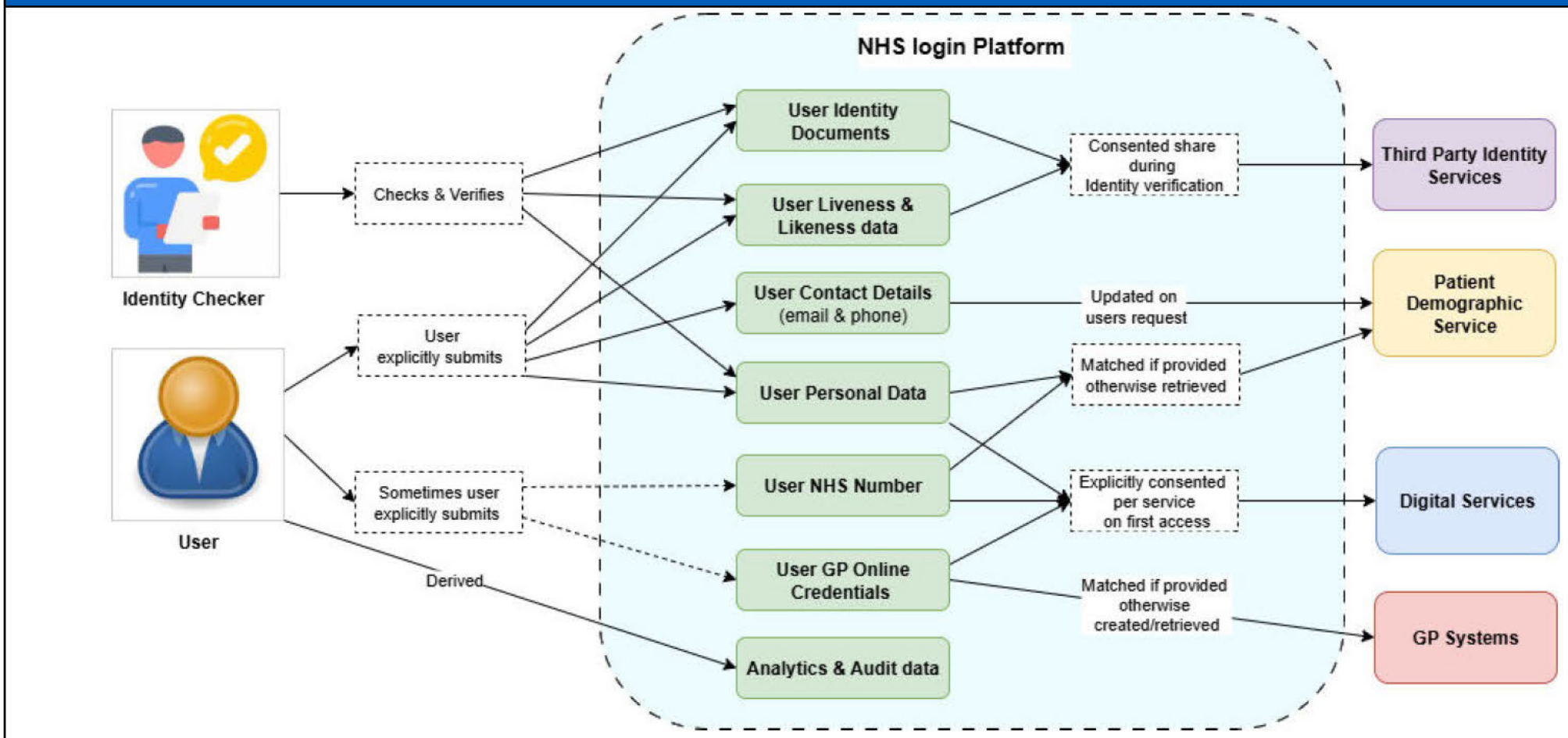
NHS login has over 130 connected services. These are health and adult social care digital services (both internal and external to NHS England), commissioned by the NHS, that rely on NHS login to enable a user to connect safely and securely. Under the NHS login Directions 2021, all these digital services must be assessed by the Partner Integration Board (PIB) as being beneficial to health and adult social care services in England and to the recipients of health and adult social care services provided in England. In effect, NHS login confirms for a connected service that it is dealing with the correct person. The team actively seeks feedback from connected services via the Partner Collaboration Forum and the NHS England Supplier Reference Group to improve:

- **Registration, verification and authentication journeys**
- **User experience and accessibility**
- **Integration, efficiency and reliability.**

5. Data Flow Diagram(s)

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

NHS login Overview



6. Purpose of the data processing and data controllership

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

The aim of the NHS login service is to enable a user to access and manage personal data about their health, and, where applicable, their adult social care, securely through the provision of identity (ID) verification and authentication services. These ID verification and authentication services are based on DAPB3051 and the Good Practice Guides (44 and 45) issued (jointly) by the Cabinet Office and Government Digital Service.

The purposes of the processing are to:

- Verify a user's identity
- Authenticate a verified user so that they can access the service(s) to which they wish to connect in a secure manner.
- Enable the analysis of information collected in the course of the operation of the service, including by reference or linkage to other data held by NHS England, to monitor and improve the delivery of the service and other NHS England services.
- Provide statistical data to commissioners (organisations that buy health and adult social care services) and policy teams in order to achieve positive health and adult social care outcomes.

Data Controllership

Purpose	NHS England	Secretary of State	GP Practices	Healthcare and Adult Social Care Providers
ID Verification and Authentication Service*	**Yes**	**Yes**	**No**	**No**
End User Organisation**	**No**	**No**	**Yes****	**Yes****

* NHS England is a Joint Data Controller with the Department of Health and Social Care (DHSC) for the personal data it processes for the purposes of NHS login. Users of NHS login are informed about the processing of personal data about them through the Privacy Notice[2], Terms and Conditions[3] and Cookies policy[4].

**Connected services act as data processors on behalf of the end user organisation who are data controllers. Multiple end users may use a connected service but are sole data controllers for the data related to their area and users. An end user organisation may be a GP or health or adult social care provider.

[2] https://access.login.nhs.uk/privacy

[3] https://access.login.nhs.uk/terms-and-conditions

[4] https://access.login.nhs.uk/cookies

Key Benefits:

- **Individuals save time** by not having to physically attend an NHS site for identity verification to access digital health and adult social care services and by having one login that can be used across multiple services.
- **Individuals have greater trust** in digital tools and services offered by the NHS and adult social care providers, as access is secured through a robust and consistent process.
- **Improve uptake and adoption of digital health and adult social care services** by making service adoption for individuals simple by providing a single and consistent way of accessing multiple digital health and care service.
- **Reduce burden on health and adult social care providers care** by providing capabilities that enable patients to self-manage their health and access online health and care services without having to present themselves physically at a health service location.
- **Ensure patient personal data is protected to a consistent level** through provision of a trusted process and supporting technical services for verifying and authenticating identity to a consistent level that meets defined standards.
- **Improve efficiency, increase interoperability, and reduce costs and time to market of online health and adult social care services** by providing identification services that can be re-used so that service providers do not have to deliver identity services themselves.

7. Description of the Processing

Nature of processing

Source of data and method of collection
Personal data processed by NHS login services will be provided: • by the user, irrespective of the service used by the user. • by the Personal Demographic Service (PDS) • by the National Proxy Service (NPS) • by GP Systems • by His Majesty's Passport Office
Users
Personal data is collected from users from the point they create an NHS login account. Users provide: • Email address (verified through a secure link) • Mobile or landline number (verified via One Time Passcode) • Demographic information (for P5 and P9 journeys) Depending on the identity verification level (P0, P5, P9), a user may also submit: • A photo ID document • A passport number • A live facial scan or a short video for liveness/likeness checks Users may optionally take part in surveys, interviews, or user research, and may accept analytics cookies which collect performance data about how they use the service. If a user encounters a technical issue, they may submit details through an online help form.
Authoritative NHS and Government systems
Certain personal data is collected by querying secure, authoritative datasets to confirm identity or link users to their NHS records: • Personal Demographics Service (PDS) – demographic matching and retrieval of the NHS number • National Proxy Service (NPS) – for retrieval of associated proxy relationships • GP systems (EMIS, TPP, etc.) – for users verifying via GP Online Credentials or Provisioning API • His Majesty's Passport Office (HMPO) – validation of UK passport details These datasets are accessed via secure APIs or, in specific cases, through manual identity checks performed by trained NHS login verification staff.

Audit and system-generated data

NHS login collects audit data automatically during use of the service, including:

- IP addresses
- Authentication events
- Verification events
- Access events
- Update events

These data are captured within the Platform Protective Monitoring function and are used for security, service monitoring, investigation, and legal compliance if required.

How data is used

The data collected is used to:

- Verify a user's identity (identity verification)
- Authenticate a verified user so that they can access the service(s) to which they wish to connect in a secure manner.
- Support and resolve user service problems
- Enable the analysis of information collected during the operation of the service, including by reference or linkage to other data held by NHS England, to monitor and improve the delivery of the service and other NHS England services.
- Provide statistical data to commissioners (organisations that buy health and adult social care services) and policy teams to achieve positive health and adult social care outcomes.

Identity Verification

Personal data is used to verify a user's identity at the appropriate verification level:

P0 (Low Identity Verification):

- User creates an account using email and phone number to verify they are in control of the email and mobile phone number
- User can access P0 services.

P5 (Medium Identity Verification):

- User completes P0 (Low Identity Verification)
- User submits demographic information to 'claim' the identity they are assuming.
- Users submitted information is 'looked' up against the information held on PDS.
- Where a successful match on PDS is made, a link between the NHS login account and NHS Number will be formed. Where unsuccessful the user will be asked to retry, and the account will remain at P0 (low).
- User can access P5 services.

P9 (High Identity Verification):

- User directed to the NHS login verification platform

- User submits demographic information, photo ID documentation or UK passport number to support the High (P9) process.
- User conducts a Liveness check.
- User conducts a Likeness check.
- User presented demographic information matched to data held on PDS.
- User matched to the record in PDS.
- User matched to the Likeness Liveness check outcome
- User can access P9 services – such as being able to order a prescription.

For P9, an individual will upload a photo and a video of themselves, replaying (spoken, signed or written) 4 numbers that NHS login provides. The video is sent back to NHS login. Alternatively, NHS login will crop the picture from the photo ID and send this to a third-party processor (iProov). As part of this, the individual completes an iProov facial check. iProov conduct a likeness check between the two photos and confirm the likeness or not. No identifiable data is sent to iProov, and an individual unique transaction number is generated to enable the confirmation to be linked back to an individual within NHS login.

Where an individual has already had their identity verified at their GP Practice and they have created a Patient Online account, an individual can uplift from a P5 to a P9 account online.

NHS login uses the records held in the PDS database as the data repository to reference a verified Identity before matching the user to an NHS Record.

Digital services that only require a Low (P0) level of verification, NHS login will verify the email address and phone number only. A lookup against PDS is not required.

More information on likeness checks and identity proofing levels is available at:
https://digital.nhs.uk/services/nhs-login/nhs-login-for-partners-and-developers/nhs-login-integration-toolkit/how-nhs-login-works

https://nhsconnect.github.io/nhslogin/user-journeys/

The manual ID checks are conducted by Home Office trained ID verification staff, supplemented with on-the-job training delivered by senior ID checkers and use of government recommended identity reference sites, including Public Register of Authentic identity and travel Documents Online (PRADO).

To support a high demand of ID verifications, NHS login has supplemented the Manual ID verification process with an 'Automated' ID verification process, where elements of the Manual ID verification process is delivered by contracted 3rd Party suppliers (for example Experian, His Majesty's Passport Office). Where suppliers are used to deliver an ID checking component, an assessment has been conducted by the NHS login DSC security stakeholder to confirm the supplier product.

Identity Authentication
Once a user has an NHS login, their data is used to authenticate them securely when accessing connected services. This includes:

- Generating and transmitting scopes and claims (identity attributes) to connected services through OpenID Connect.
- Supporting multi-factor authentication (password plus OTP or device-based authentication).
- Enabling connected services to recognise a user, create an account, or link to an existing one.

Supporting Connected Services (Digital Health and Adult Social Care Services)

Digital Services who use the NHS login service for identity verification and authentication will be connected to NHS login as part of the Assured Onboarding process. These are known as Connected Services. These Connected Services will be a Processor for NHS England, or where applicable, a Processor for the commissioner (for example a General Practice, or Integrated Care Board (ICB) or NHS Trust). Where services assert the role of an Independent Controller for the data processed, then this is subject to additional evaluation to confirm the assertion.

As part of the data flow between the Connected Service and NHS login data (scope and claims) is used to:

- Provide identity and personal information
- Pass GP Credentials*
- Allow services to access GP-held data via Interface Mechanism 1 (IM1)*

The sharing of scope and claims with Connected Services is subject to explicit user consent. If a user refuses data sharing at the point of access, NHS login prevents transmission of scopes and claims, and the service must provide an alternative non-NHS login access route.

*Connected Services requiring GP Integration Credentials must have completed Interface Mechanism 1 (IM1) integration and assurance.

Service Monitoring, Quality Assurance and Improvement

NHS login uses data to operate, monitor and improve the service:

- Audit data (IP addresses, login events, journeys) is used for security monitoring, fraud detection, incident investigation, and legal compliance.
- Analytics tools (Adobe, Qualtrics) are used only when the user opts in, enabling performance analysis and user experience improvements.
- Quality assurance processes use samples of ID checks to ensure accuracy and compliance.

User Support and Problem Resolution

When NHS login users request help:

- Contact details and issue descriptions are used to diagnose and resolve problems.
- Data may be shared internally within NHS England or with contracted partners where needed to resolve a technical issue.

Only the minimum necessary data is accessed for this purpose.

Legal and Compliance

NHS login may use and share personal data where legally required, such as in response to:

- Police or law enforcement requests
- Court orders
- Public inquiries

These disclosures are tightly controlled, recorded, and only made where there is a clear legal basis.

How data is stored

NHS login stores personal data using secure, compliant infrastructure and services operated by NHS England and contracted third-party processors. Data is stored only for as long as necessary and in accordance with strict technical, organisational, and contractual controls.

The NHS login service is hosted on Amazon Web Services (AWS), AWS is used to store service data (e.g., account data, audit logs) and to run the platform that delivers the service.

NHS login uses analytics and survey platforms to support service improvement, survey responses and associated data are stored securely within NHS England's Microsoft environment

Data associated with partner assurance activities (e.g., Connected Service information and onboarding materials) are stored securely within the NHS England corporate Microsoft environment.

Where users provide identity documents, images, videos or liveness/likeness data they are stored securely within AWS or by Third□party processors.

Level of 'High risk' processing

Under the NHS England Cloud Risk Framework, NHS login is classified as a "Data Class 5" service, which reflects the sensitivity, scale, and persistence of the personal data processed.

However, despite being a high data class workload, NHS login does *not* perform "high-risk processing" as defined by the ICO. It does not conduct large-scale profiling, systematic monitoring, or AI-driven decision-making, and all automated checks include human oversight.

Scope of processing

Nature of the data
NHS login process personal and confidential data including special category data, detail of which can be found in Section 11.
Frequency of collection
Collection will be ongoing under the NHS login Directions 2021 from the Secretary of State for Health and Social Care to support new users and services.
Number of individuals affected
The NHS login service currently has over 40 million users with a potential reach of over 60 million individuals. Data collected as part of the NHS login service is described in Section 11 of this DPIA. Each year over~5 million identity verification submissions are processed and ~2 billion authentications.
Geographical area covered
NHS login is currently available to members of the public in England, Wales and the Isle of Man.
Age range included
NHS login enables the processing of data from individuals over the age of 11 years old for P5 and P9. At P0, NHS login is unable to ascertain the age of the user. Age controls to connected services remains the responsibility of the relying party.

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

NHS login - England

Statutory Vires

Under section 254 of the Health and Social Care Act 2012 and Regulation 32 of the NICE Regulations[5], the Secretary of State for Health and Social Care has directed NHS England to provide the NHS login service: NHS login Directions 2021

Lawful bases for the processing of personal data: Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR)

Personal data

- UK GDPR Article 6(1)(a) - 'consent of the individual' where a user opts to accept non-essential cookies (which comprise personal data) or agrees to take part in user research.
- 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 login Directions 2021

Special category data

- 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'***
- 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. However online identity verification and registration processes will operate entirely at the request of the user and with full transparency – in compliance with the UK Government's Identity Assurance Principles:

https://www.gov.uk/government/publications/identity-assurance-principles-for-identity-services-in-government

NHS login – Isle of Man

The Isle of Man Department of Health and Social Care (the Department) has a duty to promote, on the Isle of Man, a comprehensive health service designed to secure improvement in the physical and mental health of the people of the Isle of Man and the prevention, diagnosis and treatment of illness, and for those purposes to provide or secure in

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

the island or elsewhere the effective provision of services in accordance with the provisions of 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 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.

Under s255 of the Health and Social Care Act 2012, NHS England has been requested by the Isle of Man Department of Health and Social Care to provide NHS login, as part of services such as NHS App, to residents of the Isle of Man:

Isle of Man Access to the NHS App Request 2021

NHS login - Wales

Digital Health and Care Wales (DHCW) is a Special Health Authority established under Section 22 of the National Health Service (Wales) Act 2006 (the 2006 Act) and by the Digital Health and Care Wales (Establishment and Membership) Order 2020 (Establishment Order).

In accordance with the Establishment Order, DHCW has been directed by the Welsh Ministers under the Digital Health and Care Wales (No.2) Directions 2021 (the 2021 Directions) to carry out functions in relation to the provision or promotion of effective digital platforms, systems and services, including arrangements for the digital collection, storage, processing, analysis, use and dissemination of health service data (being data processed for or in connection with the provision or promotion of services under the 2006 Act).

Under s255 of the Health and Social Care Act 2012, NHS England has been requested by Digital Health and Care Wales (DHCW) to provide the existing England NHS login service as an authentication and identification method for residents of Wales to access digital health services: NHS login for the NHS Wales App Request 2022

DHCW has also requested NHS England to provide the NHS login service as an authentication and identification method for residents of Wales to access services delivered by third party suppliers on behalf of health providers in Wales (Third Party Connected Services). This is known as the NHS login for health services supplied by third party Apps in Wales Request 2024.

National Data Opt-Out (England)

NHS login processes personal information solely for the purposes of identity verification and enabling access to NHS digital services. The data processed is not used for research, planning, or any secondary purposes beyond individual care. Therefore, the processing activities carried out by NHS login fall outside the scope of the National Data Opt-Out.

9. Demonstrate the fairness of the processing

Fairness and Transparency
The NHS login service considers the impact of its processing on individuals by designing its journeys to be intuitive, proportionate, and accessible, ensuring users are not unfairly denied access. The service handles personal data only in ways users would reasonably expect, given that rigorous checks are necessary to protect access to highly sensitive health and adult social care information and uses only the minimum data needed. The NHS login service maintains transparency by clearly explaining how data is processed through the Privacy Policy, Terms and Conditions, and publicly available materials, ensuring individuals are not deceived or misled when their data is collected.
Lawful basis
All data processing is conducted under a lawful basis in line with UK GDPR. (set out in Section 8).
Security
NHS login makes use of robust security measures to ensure smooth operation and data security (set out in Section 17).
User rights
User rights regarding their personal data, including access, rectification, and objection (set out in Section 16).

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

Privacy Policy
The NHS login privacy policy provides the details of the processing of personal data for the purposes of the programme. It is updated from time to time, and past versions are kept to record the evolution of the policy. • Your Privacy on NHS login In addition, NHS login has a specific Cookies Policy: • Cookies on NHS login NHS login presents its Privacy Policy and Terms and conditions upon the user starting the registration process. When NHS login is used by a connected service, the NHS login programme has previously onboarded that connected service through an assurance process. In the interests of transparency, users who are signed in to the connected service by NHS login are asked, on the first occasion, for their agreement to share the relevant scopes and claims with the connected service and are made aware of the need to consider the terms and conditions, privacy policy and cookie policy for both services so that they are clear on the way their personal data are being processed by each data controller.

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

Justification for the collection and processing
The collection and processing of personal data by NHS login is necessary, proportionate, and legally mandated to deliver a secure, trusted, and nationally consistent digital identity service for health and adult social care. NHS England is directed by the Secretary of State under section 254 of the Health and Social Care Act 2012 and associated Directions to provide NHS login as the national identity verification and authentication service for health and adult social care services. Without collecting and processing the required personal data, NHS England cannot fulfil this statutory obligation. NHS login provides a secure method for users to prove their identity to access sensitive health and adult social care services. To correctly match individuals to NHS records, prevent impersonation, and prevent access to another person's confidential clinical information, NHS login must process demographic information, contact details, NHS number, identity documents or passport details (P9), biometric liveness/likeness checks and GP Online Credentials Once a user is verified, NHS login must process personal data to authenticate users securely and enable them to sign in, access Connected Services and pass consented scopes and claims to the Connected Service. For security, service stability, accountability, and quality improvement, NHS login must process audit data (IP address, login events, journey data), system logs, optional analytics (where users opt in), user research feedback (consented) and technical information necessary to resolve incidents or user issues

Data categories	Justification
Personal data	
Name	First name and surnames will be collected for each user so they can be accurately matched to their record in the PDS. This field is one of the 'mandatory fields' on which the PDS look up is based in order to find an NHS record for a user. A middle name may be processed where it is included within the ID document or supplied by the user.
Address	The address is processed during the ID document check where it is contained within a document supplied by a user (such as a UK driving licence).
Postcode	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 PDS record.

Data categories	Justification
Mobile/Landline Phone Number	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 login account. Where a user's mobile and/or landline phone number has been authenticated by the user, NHS login may use this phone number, alongside GP Online Credentials, to enable the matching of a user to the record held for them in the PDS.
Email Address	An email address will be used as a part of the authentication credentials the user has to access the NHS login service.
Date of Birth (DOB)	DOB will be collected for each user so they can be accurately matched to the record held for them in the PDS.
Age	This can be derived from an identity document supplied by a user/delegated individual.
Sex	This can be stated in, or, in some cases (such as the UK driving licence), derived from, an identity document supplied by the user.
Gender	This may be derived from the subset of information contained in the passport/driving licence and when the user submits a photo/video selfie. It may also be inferred when the user undertakes a facial scan or submits a short video.**Error! Bookmark not defined.**
NHS Number	A user's NHS number will be matched against or sourced from the PDS during the ID verification process. This is required to match a user against the record held for them in the PDS. A user's NHS number may also be sent to a connected service that the user accesses once they agree to share it as an element of any relevant scopes and claims.
GP/Patient Online Credentials (including ODS code)	GP Online Credentials may be utilised to verify and match the user to a record.GP Online Credentials may be entered by the user or retrieved via the NHS App Middleware (NAM) by the NHS login service during the ID verification process.
Official Identity Document Unique Identifier	An official identity document identifier may be submitted by the user to validate their identity or be stated in, and read from, the official identity document during the ID verification process.
Physical Description	This is apparent in any photograph, facial scan or short video supplied by the user during the verification process.
Online Identifiers e.g. IP	Audit/event logs of user activity will be generated and will contain the IP address(es) from which a user access the NHS login service. These logs

Data categories	Justification
Address/Event Logs	will be stored securely within the Platform Protective Monitoring function; these logs may be utilised, exceptionally and on an ad hoc basis, for investigative, audit and legal requests.
Cookies	The NHS login service uses essential and non-essential cookies. The essential cookies are strictly necessary to ensure the proper functioning of the service. NHS England seeks the consent of the user to the placement of non-essential cookies on their device(s). The non-essential cookies are in relation to optional analytics. These optional analytics cookies collect performance data about how NHS login is used by its users. This information is then used to develop, and improve, the service. Users are made aware of all the cookies used by the service as they are listed within the Cookies Policy for the NHS login service.
Authentication	For the purposes of multi-factor authentication, NHS login will process passwords, one-time-passcodes 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	The details of Proxy relationships and corresponding proxy subject details, proxy unique reference, NHS Number(s), may be sent to Connected services. Proxy relationships and associated access permissions will be established by the National Proxy Service.
Audit Data	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	Analytics provide data that can be used to measure the performance and success of the service and are used to improve performance and user experience.
Special category data	
Racial / Ethnic Origin	Images submitted during identity verification may contain visible characteristics; however, NHS login does not use these images to infer racial or ethnic origin and does not carry out any processing that would treat individuals differently on that basis. Therefore, no special category data relating to racial or ethnic origin is processed
Biometric Data (Fingerprints / Facial Recognition)	Facial images captured through a video selfie and facial images cropped from identity documents (passport/driving licence), plus derived biometric comparison data (e.g., liveness indicators and likeness-matching metrics).

Data categories	Justification
	The data is captured to ensure the user is a genuine, live individual and that their facial image matches the photograph in the identity document, enabling high-assurance (P9) identity verification. No biometric templates or long-term biometric profiles are created or retained.

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

Identity Verification

During the NHS login identity verification process, personal data supplied by the user is referenced and matched against authoritative datasets to confirm identity:

- Personal Demographics Service (PDS) – demographic data is matched to correlate identity and retrieve and match to the user's NHS number.
- GP/Patient Online (POL) credentials – for users uplifted from GP-created credentials, the information provided is matched to the PDS record.

This matching is essential to establish verified identity and assign the correct NHS record.

Certain components of ID verification are delivered through third-party suppliers, as part of these component processes:

- Identity documents may be validated against known templates or trusted datasets
- Liveness and likeness checks compare user-submitted images or video with images extracted from documents

Connected Services (e.g. NHS App)

When a user logs in to a connected service such as the NHS App, their identity (as verified by the NHS login service) is used to link them to clinical information held for example by GP or hospital systems. The data shown to the user is controlled by the data controller for that service (e.g., GP practice, NHS Trust).

NHS login does not access or process clinical data; it only provides the identity layer used to link the user to their records.

Analytics

NHS login analytics data may be combined with other NHS England datasets for the purpose of:

- Monitoring service performance
- Service planning and improvement
- Supporting Federated Data Platform (FDP) analytical use cases

This linkage is limited to aggregated or pseudonymised datasets where possible, and always within NHS England governance controls.

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

Relevant data scopes and claims from the NHS login service, following a user's agreement to share them on the first occasion, will be shared with a Connected Service to enable the user's access to that connected service.

NHS England has contracted with several third parties to deliver components of the NHS login service. Personal data about users will be shared with them as necessary to enable the delivery of those components of the service.

Personal data relating to NHS login may be shared with various other third parties on an ad hoc basis. Usually, this will be in response to a valid, and legitimate request by such a third party often, where NHS England is under a legal obligation to comply with the request.

Further information regarding NHS England's legal obligations:

https://transform.england.nhs.uk/information-governance/guidance/sharing-information-with-the-police/

https://www.england.nhs.uk/long-read/safeguarding/

Arrangements in place

A connected service that wishes to use the NHS login service has to complete the NHS login onboarding process:

https://digital.nhs.uk/services/nhs-login/nhs-login-for-partners-and-developers.

This process has been designed to assess the suitability of the connected service as a partner to the NHS login service, including its benefit to a user, and considering its readiness in terms of cyber security, technical architecture, clinical risk, and information governance.

A connected services is bound to NHS England by contractual arrangements included in a Connection Agreement and the End User Terms (where applicable) and this documentation contains provisions concerning data protection.

Where scopes and claims are shared with a Connected Service external to NHS England, NHS England remains the data controller for the personal data contained within them. The connected service is a data processor (only) in respect of such personal data. Once the NHS login activity is complete, any data subsequently processed by the Connected Service will be processed in line with the relationship it has with its own customers (i.e., end user organisations), and the Connected Service will normally act as a processor, or where applicable, a controller.

These roles and responsibilities are set out in the Connection Agreement. As part of the onboarding process, each Connected Service must confirm that these controller and processor positions are accurately reflected within its own privacy policy.

A user will be asked to confirm their agreement to the sharing of relevant scopes and claims with a connected service external to NHS England on the first occasion. Where a user declines the sharing of the relevant scopes and claims, the connected service is obliged to signpost an alternative way of accessing the service to the user (i.e. the option(s) for accessing the service without using NHS login).

Where third parties are processing personal data on behalf of NHS England, and under its instruction, as data processors to a data controller, to assist with the delivery of the NHS login service, the contractual arrangements include the provisions required by Article 28.3 of the UK GDPR. Under the contractual arrangements, any data processor engaging with a sub-processor to carry out some part of the commissioned work must impose the same data protection obligations on that party (as per Article 28.4).

14. Describe how long personal data is retained

Category of information	Retention method	Retention period
Accounts (level P0 and P5) **(Not used within a 24-month period)**	Automated system deletion after inactivity	**30 days** • the user will be contacted to inform of inactive use. • the account will be disabled and deleted if the account does not become active 30 days after user notification.
Accounts (level P9) **(Not used within a 24-month period)**	Automated system deletion inactivity	**10 years** • the user will be contacted to inform of inactive use every 12 months. • the account will be disabled and deleted if the account remains inactive for 10 years. The 10-year period is in alignment with other forms of formal identity verification i.e. passports and removes the burden of identity verification on users that do not need to regularly access digital health and care services.
Accounts (all levels) **(User deletion)**	Secure deletion, user confirmation	If the individual wishes to delete their account, they can use the Account Management feature in the NHS login service, however, once this is done, the Account is completely deleted, and the user would have to register with the NHS login service again if they wish to use the service. The account deletion feature only removes the account held by NHS login; it does not delete the data items referenced below:

		- identity evidence - log data - audit events
Identity Evidence	Secure deletion, system, and data processor confirmation	**6 months** after the account is submitted, in order to resolve any complaints, queries or challenges about inappropriate or fraudulent access. All identity evidence processed by NHS login third party data processors is purged within 90 days as per contract.
Log Data	Secure storage, automated deletion	**1 year** after the action was logged
Audit Events	Secure storage, restricted access, automated deletion	**8 years** from the event occurring – audit events use log data as the source to provide awareness to NHS England skilled security. The audit logs held will have information such as surname, first name, dob, IP address, NHS Number. The audit logs, in its current guise, will allow NHS login to see who did the verification and who the individual was who provided the supporting evidence.
Scopes and Claims Shared with a Connected Service	Secure deletion and data processor confirmation	**For the lifetime of the connection agreement –** secure deletion to be confirmed on the termination or expiry of the connection agreement

15. 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 login ensures the accuracy and currency of personal data collected directly from users through a combination of technical validation, cross-checking with authoritative datasets, and user-controlled updates, including:

1. Validation at the point of collection

Personal data provided by users (e.g., email address and mobile number) is verified through secure mechanisms:

- A securely signed URL link is sent to the email address.
- A One Time Passcode (OTP) is sent by SMS to the mobile number.

These steps confirm the user is in control of the contact details they provide and supports accuracy and non-repudiation at the time of data entry.

2. Cross-reference against authoritative sources

To ensure identity information is correct, NHS login matches the data supplied by the user against the Personal Demographics Service (PDS), which holds the NHS-wide authoritative patient record.

Where a match cannot be made, the user must recheck or re-enter their details before proceeding or seek rectification in person at their GP practice. This prevents inaccurate data from being registered.

Where a user enters a UK passport number, the details will be validated against His Majesty's Passport Office (HMPO) data. Where a match cannot be made or does not correlate with the record held within PDS the user must recheck or re-enter their details or provide an alternative identity document.

3. Use of verified GP credentials (where applicable)

Where GP Online Credentials are used for the purpose of NHS login identity verification, they support accurate matching to the record held in PDS, helping ensure demographic information aligns with clinical system records.

4. User ability to keep details up to date

Users can update their own contact details (email address and mobile number) via the NHS login User Account Management function.

This ensures their NHS login authentication information remains current and if requested to be updated by the user the contact details held within their PDS record.

5. Secure storage and controlled access

All personal data is stored securely within NHS England systems, with strict access controls and processes. This ensures that when updates occur, either by the user or via authoritative sources, they are applied correctly and safely.

6. PDS updates reflected in NHS login

Because NHS login references PDS for identity matching, any updates a user or the NHS makes via their GP or NHS records (e.g., change of name, change of GP (ODS code), change of address and death status) are reflected the next time the service checks PDS.

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

To exercise their data subject rights, users are advised to send their query to england.dpo@nhs.net

Individual's Right (to)	How they are made aware of it
Be Informed	The NHS login Privacy Policy, Cookie Policy and the Terms and Conditions are made available to a user during the registration process. An 'acceptance tick box' will be presented to the user during the initial registration and when there are any changes to these documents.
Restriction of Processing	Where an individual submits a request to restrict the processing of personal data about them under Article 18 of the UK GDPR, the request will be considered on a case-by-case basis by the Data Protection Officer team with oversight from the Data Protection Officer or their delegate.
Access	Users will be able to request a copy of their personal information by submitting a subject access request (SAR). The privacy policy contains a link through which the user can access a SAR form. The request will be handled by the Data Protection Officer Team, with oversight from the Data Protection Officer or their delegate. A reasonable and proportionate search for personal data will be undertaken by the NHS login team for consideration, review and approval by the Data Protection Officer Team.
Rectification	A user may request that inaccurate personal data about them be rectified by NHS England. Any request will be considered on a case-by-case basis by the Privacy, Transparency and Trust team with oversight from the Data Protection Officer or their delegate.
Erasure	A user may request that personal data about them be erased by NHS England. Any such request will be considered on a case-by-case basis by the Data Protection Officer team with oversight from the Data Protection Officer or their delegate. However, as the right to erasure is not absolute, and does not apply 'to the extent that processing is necessary for compliance with a legal obligation which requires processing under domestic law or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller' - which is operative in the case of NHS login due to the legal obligation created by the NHS login Directions 2021 – only personal data collected, and used, under the lawful basis of consent will be liable to erasure. Accordingly, any such

	personal data will relate to any participation by the user in user research activities or their acceptance of optional analytics cookies. Accordingly, where a request for the erasure of all personal data processed by NHS England for the purposes of the NHS login service is received from a user, the scope of the request will be limited to any personal data collected and used under the lawful basis of consent. In these circumstances, the Service Management team will liaise with colleagues working in the user research team and technical teams to establish whether any such personal data are being processed in the case of the requester, and, where that is the case, will arrange for their erasure. The results of the searches for personal data liable to erasure will be confirmed to the DPO team in order that they can communicate a response to the request to the user.
Data portability	In line with Recital 68 of the UK GDPR, the right to data portability is not applicable to the processing of personal data carried out by NHS England for the purposes of the NHS login service, the processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller.
Object	Due to the way in which it is framed in the UK GDPR, the right to object is not applicable to the processing of personal data carried out by NHS England for the purposes of the NHS login service.

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

NHS England
NHS login is has completed a compliance registration entry, in the NHSE compliance portal. This submission captures how the programme adheres to NHS England security controls library and control requirements. Any elements of non-compliance identified in the compliance portal submission are recorded in the issues register and managed accordingly to ensure delivery of a cyber resilient service.
Connected Services
Connected Services connect to NHS login to deliver health and social care services. These Services are bound by UK GDPR compliant contracts. Each Service 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. • Suppliers are required to participate in assurance activities that relate to the security of the service. Services must demonstrate compliance against various industry recognised and NHSE defined technical policies and standards.

18. Where personal data are stored or processed

The boundary of the data flow diagram set out at Section 5 of this DPIA is the UK and the European Economic Area.

All the current suppliers to the NHS login service are identified in Annex A.

To manage risk, and to eliminate costs relating to due diligence, the NHS login programme has a policy position of restricting the processing, including storage, of personal data shared with connected services (i.e. relevant scopes and claims) to locations with UK adequacy regulations. This means that the standard of data protection provided in a processing location outside the UK should be not materially lower than that in the UK.

The connection agreement is the means of imposing a geographical restriction – which, dependent on the technical architecture of the connected service, might be to the UK only, the European Union or the European Economic Area, or a specific location(s) with UK adequacy regulations.

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

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk[6]	Residual risk[7]	Measure approved (Name and Date)	Actions integrated back into project plan
1	**As a result of** technical resilience failure (cloud outage, system failure, or cyber security incident), **there is a risk that** NHS login service is unavailable, **which could lead to** users not being able to access digital services to undertake key health and adult social care transactions, including the accessing of health and social care records about them or their prescription information, causing impact to, or delayed management of, their health or adult social care. **Type of risk:** Clinical, Reputational, Operational, Cyber Security, Public Trust	**High**	High durability, scalability, security, resilience, and availability of service, by design on AWS cloud. Regular security testing and assessment against best practice.	Treat	**Low – although risk is reduced by the measures, service unavailability remains a risk**	[redacted] Deputy Director of Delivery (NHS login) – October 2025	Monitor the transactions volume and scale as required using the AWS cloud capability effectively. NHS login onboarding process checks that connected services have resilient access mechanisms outside of login. Ensure resilience and backup of the NHS login service in line with the Business Continuity Plan. In the event of service unavailability, signpost to offline routes through Connect Services. Ensure annual penetration testing and continuous security and performance

[6] Tolerate, Terminate, Treat or Transfer
[7] Low, Medium or High

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk[6]	Residual risk[7]	Measure approved (Name and Date)	Actions integrated back into project plan
							monitoring to prevent service unavailability. Ensure NHS login service aligns to NHS England Red Lines including for example disaster recovery immutable back-ups.
2	**As a result of** there being undue delay in responding to a data protection incident raised by a user due to an internal process failure or an inability to action the user's report, **there is a risk that** NHS England delays an investigation, assessment of the incident within appropriate timeframes, and, where applicable, the reporting of a personal data breach to the Information Commissioner's Office (ICO) within 72 hours as required under the UK GDPR. **which could lead to** a breach of ICO reporting requirements, GDPR requirements, reputational damage, and financial loss. **Type of risk:** Data Protection, Legal, Reputational, Financial, Operational, Public Trust	High	Robust incident management processes, clear escalation routes and ways of working between the NHS login and DPO teams. Regular staff training. Ensure automated reminders for incident deadlines and regular audits of incident logs. Monitor compliance with the 72-hour reporting requirement to the ICO. Contractual requirements in relation to prompt reporting imposed on data processors.	Treat	**Low** - Incident management processes and training reduce risk, but human error or process gaps may remain.	[redacted] Deputy Director of Delivery (NHS login) – October 2025	Incident management procedures, staff training, and compliance monitoring.
3	**As a result of** the potential for a connected service processing personal	High	Enforce strict contractual clauses, system controls, conduct regular audits, and	Treat	**Low** - Contractual controls, audits, and monitoring help, but	[redacted]	Connected service audits, contract

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk[6]	Residual risk[7]	Measure approved (Name and Date)	Actions integrated back into project plan
	data in breach of the requirements set out in the connection agreement, **there is a risk of** personal data being exposed or disclosed to parties with no legitimate entitlement to them, **which could lead to** breach of confidentiality, reputational damage, regulatory fines and potential financial loss. **Type of risk:** Data Protection, Legal, Confidentiality, Reputational		require evidence of compliance.		risk remains if controls are not enforced	Deputy Director of Delivery (NHS login) – October 2025	enforcement. Vector of trust system controls
4	**As a result of** an identity checker (human) error, **there is a risk** that a user could be matched to the wrong NHS record, **which could lead to** a personal data breach and a loss of confidentiality in respect of the personal data about the health and adult social care of the person who had been misidentified as the user. **Type of risk:** Data Protection, Confidentiality, Legal, Confidentiality, Reputational, Financial	High	Regular system audits, and error reporting mechanisms. Implement manual review for flagged cases and continuous improvement of data matching and identity verification. Manual review for flagged cases, user education on reporting mismatches, continuous improvements of both manual and automated likeness check to validate matches accurately. Continual security improvement of the process	Treat	**Low** - Robust ID verification and regular audits reduce, but do not eliminate, the risk.	[redacted] Deputy Director of Delivery (NHS login) – October 2025	Implement validation and review processes (audit). Conduct regular training and ensure all personnel are aligning to latest protocols. Support and enable users to raise incidents and issues relating to mis verification via the NHS login service help desk.

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk[6]	Residual risk[7]	Measure approved (Name and Date)	Actions integrated back into project plan
			and procedures, including training of ID checkers. Two-person rule for advanced PDS searches. In the event of a mismatch reported by a user, the implementation of a patient confusion protocol by the Service Management team with the aim of promptly remedying the position for both affected parties (i.e. the user and the mis verified person).				
5	**As a result of** access control failure and/or privilege abuse, which could lead to loss of data integrity and confidentiality, **there is a risk of** personal data being re-purposed directly or indirectly, for malicious use/gain, **which could lead to** a loss of data, integrity and confidentiality of the NHS login service and potential data breach. **Type of risk:** Data Protection, Confidentiality, Legal, Operational, Behavioural, Reputational, Financial	**High**	Granular, role-based access control, logging, monitoring & auditing. Privileged identity management. Require annual completion of Acceptable Use Policies. Conduct regular audits and provide whistleblowing channels for reporting misuse.	Treat	**Low** - Access controls, monitoring, and disciplinary policies reduce risk, but cannot remove it entirely.	[redacted] Deputy Director of Delivery (NHS login) – October 2025	Access control and monitoring through NHS England and NHS login system and platform controls.

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk[6]	Residual risk[7]	Measure approved (Name and Date)	Actions integrated back into project plan
6	**As a result of** the information NHS login references within PDS being outdated or incorrect, **there is a risk of** a mismatch of a user to an incorrect NHS record, **which could lead to** a personal data breach and a loss of confidentiality in respect of the personal data about the health and adult social care of the person who had been misidentified as the user. **Type of risk:** Data Protection, Confidentiality, Legal, Reputational, Financial, Data Integrity	High	Direct synchronisation to PDS data. PDS to implement data quality checks and provide mechanisms for users to update their information. Strong processes for PDS record matching. Monitor and reconcile discrepancies proactively. In the event of a mismatch reported by a user, the implementation of a patient confusion protocol by the Service Management team with the aim of promptly remedying the position for both affected parties (i.e. the user and the mis verified person).	Treat	**Low-** Strong controls reduce the risk but do not eliminate it.	[redacted] Deputy Director of Delivery (NHS login) – October 2025	Strict PDS matching controls, PDS quality data improvements.
7	**As a result of** suppliers acting as data processors on behalf of NHS England, **there is a risk of** them using personal data for their own purposes, **which could lead to** a contravention of the data protection legislation, a loss of confidentiality and their breaching of contractual terms.	High	Contractual controls, regular audits, and mandatory compliance with data protection standards.	Treat	**Low-** Data processing agreements and audits reduce risk, but supplier behaviour can't be fully controlled.	[redacted] Deputy Director of Delivery (NHS login) – October 2025	Contractual enforcement and audits.

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk[6]	Residual risk[7]	Measure approved (Name and Date)	Actions integrated back into project plan
	Type of risk: Data Protection, Confidentiality, Legal, Reputational, Public Trust						
8	**As a result of** users of connected services not being clear as to how personal data about them are processed by a connected service, **there is a risk of** there being a lack of transparency to the user, **which could lead to** trust issues, unintentional user agreement to the sharing of relevant scopes and claims to the connected service, and a degree of reputational damage. **Type of risk:** Public Trust, Reputational	**Medium**	Clear privacy notices, transparency measures (such as the use of an interrupt screen requesting user agreement to the sharing of relevant scopes and claims with a connected service on the first occasion) and, incrementally, through user familiarisation with this feature of the connection process. Ensure regular review of policies to ensure relevance, accessibility and understanding.	Treat	**Low** - Improved user communications and transparency measures reduce risk.	[redacted] Deputy Director of Delivery (NHS login) – October 2025	Maintain transparency and user communication.
9	**As a result of** the NHS login service relying on the connected service to control age restrictions, **there is a risk of** underage users accessing the connected service, **which could lead to** legal and ethical issues. **Type of risk:** Legal, Ethical, Data Protection	**Medium**	Introduce Gillick based age controls and assure as part of connected service onboarding.	Treat	**Low** – Age controls reduce the risk	[redacted] Deputy Director of Delivery (NHS login) – October 2025	Age control implementation within the NHS login service, preventing children aged 11 years and under verifying their identity (done) and data monitoring. Responsibility for age controls reliant and owned by Connected Services.

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk[6]	Residual risk[7]	Measure approved (Name and Date)	Actions integrated back into project plan
10	**As a result of** NHS login providing point in time data for analytics and reporting, **there is a risk of** that downstream system or service eligibility and/or decisions are made incorrectly **which could lead to** inaccuracies and a potential loss of benefit/service to the individual. **Type of risk:** Data Quality, Operational	**Medium**	Regular data refresh cycles, data quality monitoring, and user feedback mechanisms.	Treat	**Low-** Data quality controls and regular updates reduce risk.	[redacted] Deputy Director of Delivery (NHS login) – October 2025	Refresh and monitor data quality. Implement real-time data dashboards.
11	**As a result of** connected services based in England offering their service with NHS login to residents of a Devolved Administration without proper legal controls, **there is a risk of** unauthorised data processing, **which could lead to** legal violations. **Type of risk:** Legal, Data Protection, Compliance	**Medium**	Legal review and controls, restrict data flows if required, and ensure local compliance through connected onboarding processes.	Treat	**Low -** Legal reviews and contractual controls reduce risk, but cross-administration issues may persist.	[redacted] Deputy Director of Delivery (NHS login) – October 2025	Implement Provision of Services Arrangements and Work Packages. Define common onboarding process. Determine whether this is possible – i.e. are partners tied to an ODS code
12	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk[6]	Residual risk[7]	Measure approved (Name and Date)	Actions integrated back into project plan
	[redacted]	[redacted]	[redacted]		[redacted]	[redacted]	[redacted]
13	**As a result of** the potential for a connecting service to process personal data about a user shared by NHS login data in or from a location without UK adequacy regulations, **there is a risk of** personal data being processed without UK Adequacy status under a materially lower standard of data protection than that in the UK, **which could lead to** data protection issues and personal data breaches. **Type of risk:** Data Protection, Legal, Compliance	**High**	Restrict processing of personal data shared with a connected service by NHS login to locations with UK adequacy regulations. Robust assurance processes and due diligence as part of onboarding activity.	Treat	**Low-** Data localisation, contractual clauses, and monitoring reduce risk, but enforcement is challenging.	[redacted] Deputy Director of Delivery (NHS login) – October 2025	Territorial restrictions and contractual controls. Assurance as part of the connected service onboarding process. Explicit agreement to a connected service processing personal data beyond the UK and outside of the EEA.

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk[6]	Residual risk[7]	Measure approved (Name and Date)	Actions integrated back into project plan
14	**As a result of** failure of controls managed by a connected services and their associated offline process, **there is a risk that** a threat actor, with a verified NHS login account, could abuse a connected service's system or leverage it for malicious purposes, **which could lead to** which could lead to a breach of NHS login data stored by the connecting service. **Type of risk:** Fraud, Cyber Security, Operational, Reputational, Legal	High	Strengthen onboarding, regular audits, and NHS fraud detection mechanisms.	Treat and Transfer	**Low** - Enhanced controls, monitoring, and incident response reduce risk, but cannot eliminate it.	[redacted] Deputy Director of Delivery (NHS login) – October 2025	Improve onboarding and fraud detection/controls and central reporting.
15	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk[6]	Residual risk[7]	Measure approved (Name and Date)	Actions integrated back into project plan
16	**As a result of** more connected services integrating with NHS login, **there is a risk that** data is collected and processed beyond what is strictly necessary for the delivery of the service, resulting in excessive or redundant personal data being held, **which could lead to** breach of GDPR principles or data misuse. **Type of risk:** Data Protection, Confidentiality, Legal, Fraud, Transparency	**Medium**	Assess each service's data requirements during onboarding. Include data minimisation checks in the Supplier Conformance Assurance List (SCAL) and onboarding checklist. Mandate completion of a Data Protection Impact Assessment (DPIA) for new integrations by internal programmes. Ensure contracts specify data minimisation and restrict use to only what is necessary for the purpose. Use technical controls (e.g. API restrictions, field-level access controls) to limit data flows. Review actual data processed by connected services against what was approved.		**Low** – risk reduced through contract and controls but not eliminated.	[redacted] Deputy Director of Delivery (NHS login) – October 2025	Include clauses restricting data collection to what is necessary. Implement API and field-level access controls to technically limit data flows. Implement API and field-level access controls to technically limit data flows. Establish ongoing audit and monitoring processes.
17	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk[6]	Residual risk[7]	Measure approved (Name and Date)	Actions integrated back into project plan
	[redacted]	[redacted]	[redacted]		[redacted]	[redacted]	[redacted]
18	**As a result of** NHS login providing data from other national sources (i.e. ODS	**Medium**	Ensure regular synchronisation (between	Treat	**Low** – contract controls and	[redacted]	Establish automated data synchronisation

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk[6]	Residual risk[7]	Measure approved (Name and Date)	Actions integrated back into project plan
	code) to Connected Services as part of the data scopes, **there is a risk that** Connected Services rely on NHS login data rather than directly from the authoritative data source (e.g. PDS) which could be outdated or inaccurate. **which could lead to** data integrity issues and incorrect Connected Service processing. **Type of risk:** Clinical, Legal, Reputational, Data Integrity		NHS login and authoritative sources (e.g. PDS data events) so that any data provided is as up to date as possible. Define and communicate clear policies that specify when Connected Services must use authoritative sources (e.g. IM1 integration) rather than relying solely on NHS login-provided data. Provide integration guidance that encourage or require Connected Services to query authoritative sources for high-risk or high-impact data fields and/or reference use within NHS login onboarding. Monitor for incidents where outdated or inaccurate data has led to errors and use these as learning opportunities to strengthen controls.		onboarding will reduce the risk.	Deputy Director of Delivery (NHS login) – October 2025	routines between NHS login and authoritative sources (e.g., Personal Demographics Service). Develop and disseminate clear policies on when Connected Services must use authoritative sources prior to automated data synchronisation or where additional data connection assurance must be provided (i.e. IM1 assurance). Monitor for incidents of outdated/ inaccurate data and use these as opportunities to strengthen controls.
19	**As a result** of the potential for a connected service to fail and become uncontactable,	**Medium**	Monitor the volumes of data flows between NHS login and connected services.	Treat	**Low**	[redacted]	Monitoring and annual reviews.

No.	Risk	Inherent Risk	Options to mitigate (treat) the risk	Effect on risk[6]	Residual risk[7]	Measure approved (Name and Date)	Actions integrated back into project plan
	there is a risk that personal data of users contained in relevant scopes and claims shared with it will not be disposed of securely in line with the requirement set out in the connection agreement and for that to be confirmed in writing to NHS England, **which could lead to** a loss of control of those personal data.		Conduct annual reviews. Issue NHS login's data destruction form to a connected service that is known to be in difficulty and chase its completion and return. Where a connected service does not return a data destruction form, issue a letter setting out the potential contractual breach to any administrators appointed in the case of a failed connected service, any successor in title, and/or the last registered address of the failed connected service. Chase a response to the letter.			Deputy Director of Delivery (NHS login) –February 2025	Destruction forms and contractual breach escalation.

20. 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)

21. 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]	IAO	[redacted]

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

22. Summary of High Residual Risks

There are **No** High residual risks.

Risk no.	High residual risk summary

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 login Third Party Data Processors and Connected Services

Third Party Data Processors	
Name	Product and/or functionality provided
Amazon Web Services	Infrastructure, platform, data hosting and liveness and likeness component
Experian/ Mitek	Identity document validation component
HMPO	UK passport validation component
iProov	Liveness and likeness components
Qualtrics	User data feedback
Splunk (Softcat)	Application that monitors the health of national live services, detecting incidents, and alerting to suspicious activities
Federated Data Platform	Analytical data from NHS login is shared for purpose of improving NHS services

Connected Services
For the latest connected services see: https://www.nhs.uk/nhs-services/online-services/nhs-login/websites-and-apps-you-can-access-with-nhs-login/

Annex B – Risk Assessment Matrix

Use the matrix below to make an objective assessment of the risks. Consider the severity of the impact and likelihood of the event occurring to assess whether the risk is high.

- **Likelihood** means how likely it is that the risk or impact of the risk may materialise.
- **Severity** means the magnitude of the risk and its impact if it materialises.

Assessing the likelihood and severity of the risks will enable you to prioritise your response to the risk – what controls you should put in place immediately to minimise the risk; what you should do soon and what you can do later, if resources allow, etc.

Severity of impact				
	Serious harm	**Low risk**	**High risk**	**High risk**
	Some impact	**Low risk**	**Medium risk**	**High risk**
	Minimal impact	**Low risk**	**Low risk**	**Low risk**
		Remote	Reasonable possibility	More likely than not
		Likelihood of harm		

Annex C – 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
Claims	Claims are individual attributes about a user—such as name, NHS number, date of birth, or verified contact details—that NHS login sends to a connected service after the user has agreed to share them. Claims are derived from authoritative sources, including the Personal Demographics Service (PDS), and are transmitted securely using OpenID Connect to allow the connected service to recognise or create a user account.
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
DPO	Data Protection Officer - A professional responsible for ensuring that an organisation complies with data protection laws and regulations
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
GP Credentials	GP Credentials (also referred to as GP Online Credentials or Patient Online (POL) Credentials) are the login details issued to an individual by their GP practice to enable access to patient-facing digital services, such as viewing medical records, ordering repeat prescriptions, or booking appointments. These credentials are created and verified by the GP practice and can be used by NHS login to support identity verification and record matching.
GPIT	General Practice IT - The systems, software, and digital infrastructure used in general practice settings
HMPO	His Majesty's Passport Office - The sole issuer of UK passports and responsible for civil registration services through the General Register Office

IAO	Information Asset Owner - A designated individual responsible for ensuring that information assets are managed and handled appropriately
ICB	Integrated Care Board – Regionally distributed NHS bodies responsible for planning and funding local healthcare services
ICO	Information Commissioner's Office - UK public body that protects data privacy and freedom of information
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)
PRADO	Public Register of Authentic identity and travel Documents Online - An online repository of security features in travel documents maintained by the Council of the European Union.
PTT	Privacy Transparency and Trust
RDDT	Regional Director of Digital Transformation - Role overseeing digital transformation within NHS regional areas
Scopes	Scopes are permissions requested by a connected service to access specific categories of user information held by the NHS login service. When a user attempts to access a connected service for the first time, NHS login presents an interrupt screen asking the user whether they agree to share the relevant data associated with those scopes. Only after the user actively agrees will NHS England transmit the requested data. Scopes operate within the OpenID Connect (OIDC) framework used by NHS login to standardise secure authentication and authorisation.
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