DAPB3051 Amd 59/2025

Identity Verification and Authentication Standard for Digital, Data, Analytics and Technology Use

Version 3.1 2/12/2025

Owner / Author	Carlos Trigoso	**Status**	Final
Programme Sponsor	Melissa Ruscoe		
		Version	3.1
Co-author	Ken Harris-Jones,	**Version issue date**	02/12/2025
Document Filename	DAPB3051 Amd 59/2025, Requirement Specification		

Document management

Revision History

Version	Date	Summary of Changes
3.1	Dec 2025	Title updated to reflect the revised scope of identity verification and authentication requirements for digital, technology, and data. Reference made to authentication use case for proxy users.
3.0	21/03/2025	Updated to include new guidance on alignment with NIST best practice guidance and requirements

Reviewers

This document must be reviewed by the following people:

Reviewer name	Title / Responsibility	Version
Carlos Trigoso	Lead Enterprise Architect	3.1
Melissa Ruscoe	Deputy Director of Delivery	3.1
Ken Harris-Jones	Head of Governance, DGAT	3.1

Approved by

This document must be approved by the following people:

Approving body	Date	Version
Data Assurance Board	02/12/2025	3.1

Contents

Glossary of Terms

The following terms and abbreviations are used throughout this standards document:

Term or Abbreviation	Definition and further information
Authentication	Authentication of a person's identity. Credentials issued and checked on subsequent visits.
Authorisation	Authorisation of a role, within the framework of recognised roles, for data access. Proxy authorisation first use case of role credentials
Child	A child is defined by the Children Act 1989 as a person under the age of 18 years. For the purposes of this standard young people (aged 16 or 17) are presumed to have sufficient capacity to make their own decisions regarding access to digital health services and to consequently decide on their own medical treatment, unless there's significant evidence to suggest otherwise. Children under the age of 16 may have capacity to make their own decisions and therefore in line with existing Patient Online guidance it is recommended that services regularly assess their capacity and to adjust any proxy access accordingly.
Clinical Authorisation	Authorising a person to access a health or care service, ensuring that no harm would be caused to that person by providing the access. May be required before a person can access a health or care service. The process may also include checking for data that is confidential to a third person and redacting harmful or third-party confidential data before access can be authorised.
DAB	The Data Assurance Board have responsibility for approving information standards, data collections and extractions (ISCEs) to be used in health and adult social care (under the auspices of DAPB)
DAPB	Holds delegated authority from the Secretary of State for Health and Care for the oversight and management of the governance and assurance framework for Information Standards, Data Collections and Extractions published in England.
Delegated access	The sharing of a person's access to digital health and care services with another person who they nominate to be able to act on their behalf. In this case both parties must have mental capacity.
Digital health and care services	A health or care service provided by an NHS or non-NHS organisation that is either wholly or partly available digitally, including social care services.
GDS	The Government Digital Service is part of the Cabinet Office and handles the digital transformation of government.
GPG44	See References section below.
GPG45	See References section below.

Health and care organisation	Any NHS or non-NHS provider, organisation, company, or authority offering health and care services including social care.
Identity Verification	Verification of identity evidence that may be presented by a person to support proving their identity.
NHS England – Transformation Directorate	The national provider of information and specification standards, data architecture, national data collection, analysis and reporting, and central IT systems for commissioners, analysts and clinicians in health and social care in England.
NIST 800-63	See References section below
Official, Nationally Held Records and Clinician Records	Official, Nationally Held Records and Clinician Records are a log and record of an individual's health and the treatment they have received from the NHS and/or registered health and care organisation, for example GP record, NHS hospital record, Private hospital record etc. These records are maintained by clinical and health professionals.
PCAG	The Privacy and Consumer Advisory Group (now known as One Login Inclusion and Privacy Advisory Group) advises the government on how to provide users with a simple, trusted and secure means of accessing public services.
Physical Comparison	Comparing the likeness of a person to trusted photo documentation that they have presented to support proving their identity. For example: a passport or driving licence.
Proxy access	The sharing of a person's access to health and care services with another person when there is a legitimate need to do so but the person is not able to take responsibility for delegating this themselves. For example: A parent claiming access to a child records, and Lasting Power of Attorney.
Registry	Where granted access is recorded and referred to, and the audit trail of who checked and granted the access.
Standalone or Patient/User Managed Records	Patient/user managed records are health data and other information related to the care of an individual that is maintained by the individual themselves, for example adding activity and vital signs from a smart device. A standalone record may be updated by an individual or clinical and health professional, and contains information relating to a single event, request or condition that is recorded outside of nationally held or clinician records, for example updating a sexual health event, or a request to update contact details.

References

The following documents are referenced throughout this document:

Ref. No.	Document Title (click for link)	Further information (click blue document titles for links)
1	GPG45	Good Practice Guide 45 "Identity proofing and verification of an individual" is a document by the Cabinet Office that provides guidance on the identity proofing and verification of an individual using online services.
2	Guidance for registered pharmacies providing pharmacy services at a distance, including on the internet	Guidance for registered pharmacies providing pharmacy services at a distance, including on the internet Sets out the requirements for distance selling and online pharmacies.
3	Standards for Online and Remote Providers of Sexual and Reproductive Health Services	Standards for Online and Remote Providers of Sexual and Reproductive Health Services sets out the requirements for the provision of sexual health services
4	GPG44	"Authentication credentials for online government services" is a document by the Cabinet Office / Government Digital Service that relates to the use of identity credentials to support user authentication for online government services.
5	GPG43	Good Practice Guide 43 "Requirements for Secure Delivery of Online Public Services", which sets out an approach to determining the necessary components to deliver public services securely online.
6	Patient Online: The GP Online Services Toolkit	Patient Online: The GP Online Services Toolkit is a document by the Royal College of GPs that summarises expert opinion and feedback explaining what online access involves, provides key messages for key stakeholder groups, and outlines future steps to support practices with Patient Online. Patient Online: The Toolkit can be found at: http://www.rcgp.org.uk/patientonline
7	Good Practice Guidance on Identity Verification for Patient Online	Good Practice Guidance on Identity Verification for Patient Online Services in Primary Care is a document by NHS England to help General Practice apply consistent good practice in identity management when providing patients

	Services in Primary Care	access to online services such as booking appointments, ordering repeat prescriptions, and viewing clinical records.
8	Working with online record access - the challenges	Working with online record access - the challenges is a toolkit of guidance by the RCGP about online records access and the impact and considerations that should be undertaken.
9	Coercion: Guidance for general practice	Coercion: Guidance for general practice is a document by the RCGP about online access to practice services and records providing new and additional opportunities for coercive behaviour, and the available measures to minimise risk to patients.
10	Countersigning passport applications and photos	Countersigning passport applications and photos is a GOV.UK online guide to the countersigning requirements for passport applications and photos.
11	NIST 800-63	NIST Special Publication 800-63 - Digital Identity Guidelines provides technical requirements for implementing digital identity services

Document Management

Version	Summary of Changes	Date
1.0	First version of the Standard	20/06/2018
2.0	Update of the Standard to clarify applicability of the standard, removal of proxy access section (specific proxy standard to be published (Autumn 2025) and provide further guidance and transaction examples for identity verification and authentication levels.	23/05/2024
3.0	Further revision, which includes NIST reference and further clarity. The document also separates authorisation protocols into implementation guidance for clarity of this identity and authentication standard, following final DAB approval.	16/04/2025
3.1	New revision to broaden the scope of the Standard as described in this version of the documentation	02/12/2025

1 Introduction

What is this standard for?

This standard provides a consistent approach to identity across digital health and care services. It describes why and how a person should prove their identity to access digital health and care services. For example: their GP practice, their local hospital, and their social care provider.

NHS England has worked on this standard in conjunction with many key clinical and privacy stakeholders including the Care Quality Commission, the Royal College of GPs, the Joint GP IT Committee, and the Privacy and Consumer Advisory Group.

The defined standards and principles, in this document, are to enable co-ordination and reduce duplication of effort. Elements considered by this standard include:

- Identity verification.
- Identity authentication.
- Authorisation and Clinical authorisation (*see* Authorisation Use Cases)
- Typical example transactions.

This standard primarily addresses identity verification and authentication requirements, for digital health and care services, accessed directly by individuals, or their authorised representatives, in primary and secondary care settings. However, the principles and requirements outlined herein should not be interpreted as defining the exclusive means by which patient data may be appropriately accessed.

Patient data is legitimately accessed by a broader range of individuals beyond the direct care provision scenarios described in this document, including, but not limited to: data processors operating under contractual arrangements with health and care organisations, research teams conducting approved studies, public health authorities performing statutory functions, and regulatory or oversight bodies exercising legal mandates. These access patterns do not constitute "services" in the sense used throughout this document but rather represent distinct data processing activities governed by separate legal frameworks and operational requirements.

Regardless of the access scenario, purpose, or category of individuals involved, all access to patient data must adhere to fundamental information governance principles that include: demonstrable "need to know" based on legitimate purpose, "minimal disclosure" ensuring only necessary data elements are accessed, "valid intent" supported by appropriate legal basis and ethical justification, "informed consent" where required by law or professional standards, and "role-based access controls" that technically enforce appropriate boundaries. These principles apply universally across all contexts in which patient data is accessed, whether explicitly addressed in this standard or not. Health and care organisations remain responsible for implementing appropriate technical and organisational measures to ensure these principles are upheld across all data access scenarios, and for maintaining comprehensive audit trails that demonstrate compliance with applicable legal and regulatory requirements.

What is not covered by this standard?

This document does not cover:

- The technical solutions or the user experiences required to implement this standard.

- Unique identifiers such as NHS number.
- Cyber security, threat detection, or other related disciplines.

Identity verification and authentication form part of a holistic approach to securing digital health and care services. A comprehensive risk-based approach to security is required, along with recognition of what threats can *and cannot* be mitigated through identity verification and authentication alone. See also GPG43 "Requirements for Secure Delivery of Online Public Services"[1].

Who does this standard apply to?

Any NHS or non-NHS provider, organisation, company, or authority that provides individuals with access to digital, data, analytics and technologies for health or care services must adhere to this standard.

[1] Requirements for secure delivery of online public services - GOV.UK (www.gov.uk)

What about other available identity standards?

This standard is intended to co-exist with other general identity standards such as GPG45 "Identity proofing and verification of an individual", and also with identity standards that exist for other specialised areas such as distance selling in pharmacies[2] and those for online and remote sexual health services[3].

Why is this standard needed?

The NHS wants to put people in control of their own health and care so that they can make informed decisions. The NHS also wants to support people such as carers and family members who need to access a person's health and care services on their behalf.

Digital health and care services contain a person's information and will allow a person to record decisions and preferences about their care that will affect them. For example: organ donation, end of life preferences, and data choices. Digital health and care services will also allow a person to record data about themselves to influence their care. For example: blood sugar levels, heart rate readings, and inhaler usage. It is therefore important that only the correct person has access.

An online identity will make it easier and quicker for a person to access online health and care services, but it must be done in a safe, consistent, and reliable manner.

The necessary security must be put in place, but without making access to digital health and care services so complex or time-consuming that people are deterred from using them.

[2] https://www.pharmacyregulation.org/sites/default/files/document/guidance_for_registered_pharmacies_providing_pharmacy_services_at_a_distance_including_on_the_internet_april_2019.pdf

[3] https://www.fsrh.org/standards-and-guidance/documents/fsrhbashh-standards-for-online-and-remote-providers-of-sexual/

What is required?

An important part of verifying a person's identity involves performing a physical comparison, comparing their likeness to trusted photo documentation. For example: a passport or driving licence. This can be done entirely online (dependent on the individual) using a laptop, smartphone, tablet, or other similar device in a convenient location. For example: at home or work.

For some people, it may not be possible to do this entirely online, and it may therefore be necessary for a person to verify their likeness to trusted photo documentation by travelling to a physical location. For example: their local hospital or their GP practice. It is anticipated that there will not be a charge for this service.

If a person doesn't have sufficient evidence to verify their identity, it may be possible for a health or social care professional who knows the person to reliably vouch for them and confirm who they are. For example: the person's GP, nurse, consultant, or social worker.

The need for digital identity

Health and care organisations require ways for people to access online services to enable more efficient diagnosis, treatment, self-care, and care of others.

Health and care organisations also have a legal requirement:

- To adhere to the General Data Protection Regulation (GDPR), Data Protection Act 2018, and other relevant legislation;
- To ensure that confidentiality is respected in relation to all health and care information accessible to members of staff (including doctors, nurses, clerical staff, and others) – to respect the common law duty of confidence and provide a duty of care.

Delivering services online has significant implications for how we deliver health and care services in future. Controls that are typically built implicitly into the healthcare process (e.g. via a GP consultation) such as trust, privacy, clinical safety and security now need to be delivered digitally.

People expect their information to be appropriately protected, but also that they can access information easily when needed.

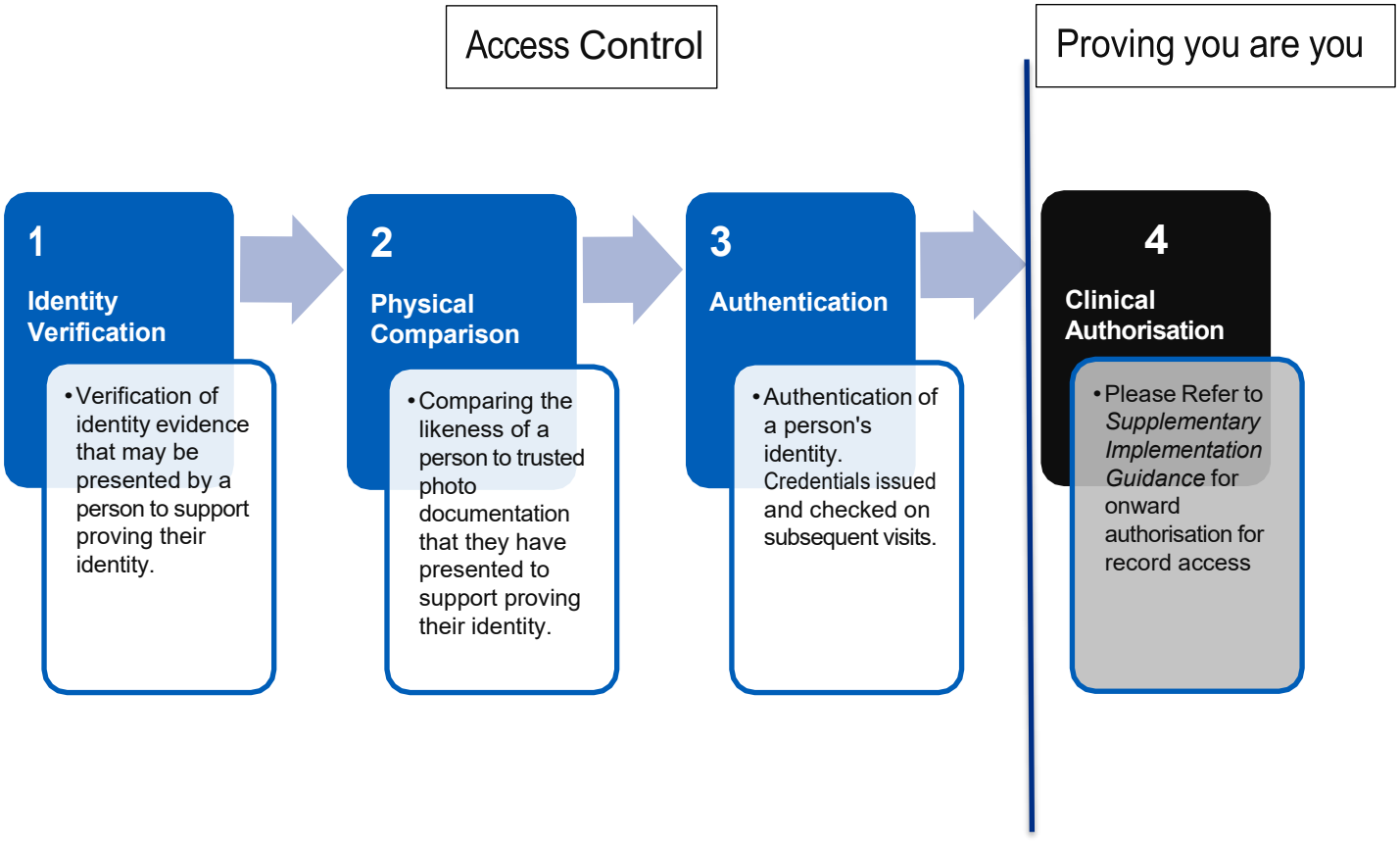
Health and care online services are distinctly different from other online services such as banking, insurance, and retail. Financial loss is potentially recoverable and insurable by financial organisations, but a person's health or care information obtained fraudulently cannot be recovered, and its unauthorised sharing and use cannot be undone.

Since any health or care information relating to an individual is considered sensitive, information held by health and care services must only be accessible online by the person to whom it belongs, or a person with delegated access (see Section 6). Controls need to be put in place to protect this sensitive information; there is a need for a person to have to prove their identity to be able to access the information using a digital health or care service. A possible solution could involve performing a physical comparison of the person and a trusted identity document that they have provided, such as a passport or a driving licence.

Where there is a need for a person to have to re-prove their identity due to lost or invalid credentials (e.g. a forgotten password, or lost phone), this must be carried out to the same standards as the initial verification; this may involve re-presenting of documentation or physical presence.

Overview of identity verification and authentication

The following diagram shows the four key steps of identity verification and authentication that are described throughout this standard below:



2 Identity verification

Identity management is a complex problem and a term that is often interpreted in different ways. Therefore, a common language is needed to reach a common understanding of the requirements. For understanding identity verification this document is based on the following terms and concepts:

- The process should enable a legitimate individual to prove their identity, in a straightforward manner, whilst creating significant barriers to those trying to claim to be somebody they are not.
- The individual shall expressly declare their identity.
- The individual shall provide evidence to prove their identity.
- The evidence shall be confirmed as being valid and/or genuine and belonging to the individual.
- Checks against the identity confirm whether it exists in the real world.
- The breadth and depth of evidence and checking required shall differ depending on the level of assurance needed in verifying that the identity is real and belongs to the individual.

A person's record at their registered GP practice may already exist, possibly going as far back as their birth, and will continue to the end of their life. Therefore, there is a requirement to bind the individual to their existing medical record.

Standard levels of assurance as identified in GPG45 are not always directly applicable to the NHS and each element within the identity verification process needs to be assessed separately.

Please also see "Appendix A – General principles for identity verification and authentication" and "Appendix B – PCAG Privacy Principles".

Requirements for identity verification

To sufficiently bind a person asserting their identity to an existing medical record, the following is required:

1. An item of official photographic identity (such as a passport or driving licence) as defined in GPG45.
2. Know that the document appears to be genuine.
3. A physical comparison between the photographic identity and the person asserting their identity, and to link the asserted identity to the medical record. Examples of ways of carrying out physical comparison may include:
    a. Being physically present at the point of identity verification.
    b. Online services which enable live comparison of the individual with photographs held on legal documents (such as driving licence or passport).
4. The individual is not deceased, by reference to an Authoritative Source such as the Personal Demographics Service[4] (PDS).

[4] https://digital.nhs.uk/services/personal-demographics-service

Face-to-face vouching

Face-to-face vouching can be used where a person does not have the appropriate photographic evidence, or in any situation in which a health or care professional meets the requirements:

1. Vouching is different to countersigning that is used for passport and driving licence applications (as detailed in Countersigning passport applications and photos[5]).
2. The objective of face-to-face vouching is to reliably link a person to an existing health and care record under which they are being treated. For example: a GP may vouch that the person requesting digital access to GP online services is the person to whom the GP record relates.
3. Only a health or care professional who has authorised access to a person's health and care record (i.e. they are trusted) can authorise the link between the record and that person via face-to-face vouching. This vouching can be delegated to appropriate staff where the individual being verified is well known to the organisation.
4. Face-to-face vouching should be accompanied by appropriate supporting evidence if it is required in the opinion of the health or care professional carrying out the vouching (examples of this supporting evidence may include utility bills, council tax bills or other items as set out in GDS Guidance How to accept a vouch as evidence of someone's identity[6].
5. Where necessary (for example the person is not well known to the staff) the vouching can be supported with clinical questions against the record, this must be carried out by clinical staff with access to the individuals medical record – see NHS England Good Practice Guidance on Identity Verification for Patient Online Services in Primary Care[7].

Please also see "Appendix C – GPG45 element scoring".

Auditing identity verification

The process of identity verification, however implemented, will need to be audited. In order to support this, information should be recorded appropriately so that it is possible to:

- Identify who carried out the identity verification process.
- Determine what Identity Evidence was presented by the Applicant.
- Determine that the evidence presented appeared to be genuine.

3 Authentication

After having their identity verified, authentication is the technical process for a person to confirm their claim of that identity each time they access an online health or care service.

This usually means 'logging on' to a system with a unique identifier (e.g. email address) and an authentication factor (e.g. password).

Generally, authentication factors fall into one of the following three categories:

[5] https://www.gov.uk/countersigning-passport-applications

[6] https://www.gov.uk/government/publications/how-to-accept-a-vouch-as-evidence-of-someones-identity/how-to-accept-a-vouch-as-evidence-of-someones-identity

[7] https://www.england.nhs.uk/wp-content/uploads/2015/03/identity-verification.pdf

1. Something the user has - such as a code sent in a text message to a mobile phone.
2. Something the user knows - such as a password or passphrase.
3. Something the user is - such as a fingerprint, or facial recognition (i.e. biometrics).

Sometimes more than one factor is required to authenticate a user, known as multi-factor authentication (MFA).

More information about user authentication can be found in GPG44.

This standard defines two types:

- Strong authentication.
- Basic authentication.

An online health or care service must assess the authentication type that best suits its security and access requirements. These requirements should depend on various risk factors such as the sensitivity of the service and the information that can be accessed and/or recorded. Refer to "Appendix D – Authentication and verification transactions" of this document for examples of transactions and an appropriate type of authentication. Other resources may also be useful, for example: the General Pharmacy Council document "Guidance for registered pharmacies providing pharmacy services at a distance, including on the internet".

Strong authentication

Equivalent to *NIST Authenticator Assurance Level 2* from *NIST SP 800-63*[8]. Strong authentication requires:

- Multi-factor authentication.
- A mechanism to prevent replay attacks.

Remembered Devices

When implementing Strong authentication, services may reduce the burden on users by implementing 'Remembered Device' functionality. After successfully authenticating the user, the service may offer the user the option to 'Remember This Device' at which point the service takes steps to allow the device to uniquely identify itself on subsequent authentication attempts. In this instance, the device becomes a 'something you have' authentication factor, negating the need for a second authentication factor during subsequent authentication. The use of this feature must be time-bound, eventually prompting the user for an additional authentication factor.

[8] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf (industry best practice)

Basic authentication

A basic, single factor, form of authentication such as the common approach of using an email address and password. This may be deemed adequate for services such as booking GP appointments.

Logout

All online health or care service must provide the facility for users to safely log out of the service and this must include safely abandoning transactions part-way through. Services must ensure that once a user has initiated such an action, no party is able to access any data related to the user or continue any transaction on their behalf without authenticating.

Technical steps required to safely log a user out could include:

- Deletion or invalidation of any unique session identifiers.
- Deletion of any data held locally on the user device (e.g. transaction data held temporarily in the browser; data stored within an installed mobile application).
- Prompting the user's device to clear any other locally held data (e.g. web browser cookies, cached web pages, etc.).

Re-authentication

All online health or care service must reauthenticate users after a period of inactivity or extended use. This is required to maintain confidence in the user's claim of a verified identity and to ensure continued legitimate access.

Whenever possible, services must prompt the user to reauthenticate immediately after the defined period has elapsed, without the need for the user to initiate an action first. (e.g. redirecting away from an open web page automatically)

Services must define the allowable periods of inactivity or extended use as short as possible relative to the risk and usability requirements of the service, aligning to the maximum durations defined within NIST SP 800-63 and based on the required authentication type defined previously:

Authentication Type	Expectation	Inactivity	Extended Use
Strong	Should	15 minutes	12 hours
	Must	30 minutes	12 hours
Basic	Should	30 minutes	12 hours
	Must	30 days	

Durations longer than those listed must only be allowed where a specific use case necessitates it in line with the usability and risk of the service.

Installed Applications

Services accessed via an installed application, such as on a mobile or tablet device may extend the period before a user must be fully reauthenticated by implementing a local authentication step to protect access to the application. Usually this would be implemented as check against a locally configured PIN or password, or a biometrics check using the device's built-in capabilities.

This is allowable under the following conditions:

- The user must complete a full basic/strong authentication process the first time they access the application.
- The user should be prompted to configure the local authentication after completing the full authentication.
- The token or identifier used to maintain the user's authentication session must be encrypted-at-rest and the decryption process dependent on the local authentication action.
- The user must complete a full authentication process at least every 30 days.
- The user must be prompted for the local authentication factor:
    - After a period of inactivity within the application.
    - Reopening the application from a background or paused state after a period.
    - Reopening the application from a closed state, regardless of the elapsed period.
- Services must define the allowable periods of inactivity or the application being in a background or paused state as short as possible relative to the risk and usability requirements of the service and aligned to the maximum durations already defined.

Installed applications that are unable to meet these conditions are subject to the reauthentication periods defined previously.

4 Issues and escalation

There must be a defined process for raising issues, such as potential or actual exposure of credentials (Password for example), such that users know how to have credentials suspended quickly.

This process must ensure that it balances the needs of protecting a person's information against the possibility of a third party maliciously denying the user access to their own records (meaning false reporting of exposed credentials).

5 We know who you are, now what?

Please refer to the supplementary implementation guidance for reference to patterns that enable services to authorise individuals based on roles and responsibilities.

This includes:

- Clinical authorisation for a person to be granted access to their records (see section 6) Authorisation patterns for proxy access (

6 Appendices

Appendix A – General principles for identity verification and authentication

The view of how the Privacy Principles established by the Privacy Consumer Advisory Group (PCAG) are met by this standard can be found in Appendix D – PCAG Privacy Principles.

The following principles have been identified for this standard:

1. NHS and non-NHS health and care settings

- Principle
  - NHS identity verification is linked together with a NHS patient record.
  - NHS identity may or may not relate to current legal identity.
- Rationale
  - The online identity created does not exist in isolation to the medical record, it is an online account bound to an existing medical record.
  - Individuals may have changed their legal name (via deed poll or marriage) without updating the name on their medical record.
- Implications
  - More robust documentary evidence, counter identity fraud checks, and valid electronic history (such as bank records) would be required to extend an NHS identity into an identity which could be used outside the NHS context.

2. Interoperability of identity between national and local solutions across health and social care

- Principle
  - Digital identities should be portable across health and social care environments.
  - Agreed open standards should be used to minimise development costs.
- Rationale
  - Re-use of identity reduces the burden on citizens using the services.
  - Open standards promote technical interoperability, reduces the cost of development and systems maintenance and reduces the barrier to entry for new identity services.
- Implications
  - Requires a common understanding and agreement on what strength of evidence and process is required to enable online accounts
  - The approach does allow flexibility, and services may choose to meet the standard in different ways
  - The framework and approval process under which new and / or different identity mechanisms are approved must also take into account the open standards in use and adoption of revised versions or new standards

3. Clinical authorisation MUST occur within the remit of each clinical data controller

- Principle
  - The data controller of the clinical record needs to identify whether there is a risk of harm to the patient and whether third parties are referred to in the record.
- Rationale
  - Each clinical data controller has a duty of care (beyond the data protection act) to ensure the safety of the patient.
  - It's not appropriate for authorisation to access clinical information to be made by an outside party or centrally.
- Implications
  - Authorisation to one digital health and care service does not imply authorisation for another, therefore each service will need its own authorisation process and registry.
  - A particular digital health or care service may decide that authorisation is not required.
  - Audit of the clinical authorisation must be possible in the local setting where authorisation has been approved.

4. Plan and build for identity service evolution

- Principle
  - Through appropriate open standards it will be possible to integrate new identity services and phase out old ones.
  - It should be possible to revalidate identity where it becomes appropriate.
- Rationale
  - Identity verification services and authentication services will change over time, older systems will become less secure
  - New secure mechanisms for verification and authentication should be approved and adopted.
- Implications
  - We must define a framework and approval process, under which new and / or different identity mechanisms can be assessed and subsequently integrated into the existing system
  - New identity services will be added to those available.
  - Older identity services will be phased out over time and mechanisms to migrate or revalidate users should be planned for.

Appendix B – PCAG Privacy Principles

	Principle	Met / Comments
1	USER CONTROL "I can exercise control over identity assurance activities affecting me and these can only take place if I consent or approve them."	Met. Identity registration and use will only be initiated by the user.
2	TRANSPARENCY "Identity assurance can only take place in ways I understand and when I am fully informed."	Met. A full audit trail to be provided to the user.
3	MULTIPLICITY "I can use and choose as many different identifiers or identity providers as I want to."	Research required to confirm whether multiplicity is valid and required in a health context balanced against potential clinical risk of multiple identities.
4	DATA MINIMISATION "My interactions only use the minimum data necessary to meet my needs."	Met. Identity information only held where necessary.
5	DATA QUALITY "I choose when to update my records."	Only within the context of the identity element of the record – rather than the health record itself.
6	SERVICE USER ACCESS AND PORTABILITY "I have to be provided with copies of all of my data on request; I can move / remove my data whenever I want."	Met, data will be removed unless required for legal purposes.
7	CERTIFICATION "I can have confidence in the Identity Assurance Service because all the participants have to be certified against common governance requirements."	Will be met - Needs further investigation dependent on the solutions being developed – the standard will not proscribe the solution.
8	DISPUTE RESOLUTION "If I have a dispute, I can go to an independent Third Party for a resolution."	Existing NHS dispute resolution mechanisms are already in place and will be used.
9	EXCEPTIONAL CIRCUMSTANCES "Any exception has to be approved by Parliament and is subject to independent scrutiny."	Existing healthcare and data protection laws are deemed sufficient and further parliamentary scrutiny is deemed unnecessary for access to health records.

Appendix C – GPG45 scoring

The objective of the authentication service is to manage specific risks within the context of health and care services, not to attain a specific level of assurance in GPG45[1]. However, NHS England has established a common terminology to discuss risk management at a generic level by working with GDS and Cabinet Office, and has achieved a consensus on how the requirements for identity verification and authentication can be mapped to the levels of assurance identified in GPG45[1].

The following table identifies the agreed standard of evidence needed for each element of identity verification as per GPG45[1].

The purpose of this section	Required score	Justification
To obtain evidence of the claimed identity ('strength') (was element A)	Documentary evidence should* include photo identification (3) *see section 3.	Identity Evidence is required to support a link to the existing medical record, rather than to create a new identity.
To check the evidence is genuine or valid ('validity') (was element B)	1	Identity Evidence is required to support the existing medical record, rather than to create a new identity.
Check that the identity belongs to the person who's claiming it ('verification') (was element C)	3	A physical comparison is required. Biometric comparison would have been possible but there is no biometric database to enable comparison.
Check if the claimed identity is at high risk of identity fraud ('identity fraud') (was element D).	n/a	The risks that this control is intended to prevent are not relevant to health. Our requirement is to ensure the NHS medical record exists and that the individual is not deceased.
Check the claimed identity has existed over time ('activity') (was element E)	n/a	The medical record existing over a period of time provides evidence of activity history. There is no further requirement to validate digital activity history.

Appendix D – Authentication and verification transactions

Work carried out in conjunction with clinical colleagues, the Royal College of GPs, the Joint GP IT Committee, and NHS England subject matter experts has identified a range of example transactions (previously known as archetypes), given in the table below.

For the purposes of the table, identity verification and authentication are explained as follows (elements referred to as previously defined):

Purpose	Level	Explanation
Identity verification	High	Identity verification requiring physical comparison in conjunction with sufficient evidence to validate it (refer to appendix C). This is elaborated in Section 3 of this standards document.
Identity verification	Medium	Identity verification which uses Knowledge Based Verification (Element C score 2) in conjunction with sufficient evidence to validate it (elements A, B, D, and E score 1).
Identity verification	Low	Identity verification which consists of self-asserted identity, and which may not relate to any legal or NHS identity. Note – Medical information captured under Low identity verification cannot be put directly into a patients NHS record. If necessary, the relevant medical information should be sent to an NHS clinician for review and that clinician could then add appropriate information to the NHS record following appropriate assessment / verification.
Authentication	Strong	Two-factor authentication as described in Section 4 of this document.
Authentication	Basic	User-selected identifier (e.g. email address) and single authentication factor (e.g. password) as described in Section 4 of this document.

All organisations should meet the same standards of verification and authentication to ensure portability (Principle 6 in Appendix D – PCAG Privacy Principles), though the mechanisms for achieving this may vary between organisations or over time reflecting the evolution of the mechanisms (general principle 7).

Record Type	Transaction Type	Transaction Examples	Verification Level	Authentication Level
Official, Nationally Held Records and Clinician Records	Patient/User Read Medical Data, Clinical Transactions and Appointments	Read from the GP and/or secondary care record. View messages from a clinician. View current and previous appointments booked. View preferred pharmacy.	High	Strong
	Patient/User Write Medical Data, Clinical Transactions and Appointments	Submit medical readings directly to GP and/or secondary care record. Order a repeat prescription. Request or grant proxy access for another individual. Manage booked appointments. Record preferred pharmacy.	High	Strong
	Patient/User Read of Demographic and Contact Details	Read contact details from the GP record (e.g. address, mobile number).	High	Strong
	Patient/User Write of Demographic and Contact Details	Update contact details directly into the GP record (e.g. address, mobile number). Register at a new GP.	High	Strong
	Patient/User Write of Data Sharing Preferences	Record data-sharing opt-out preferences.	Medium	Strong

	Patient/User Write o Research Preferences	Register interest in research participation.	Medium	Strong
Standalone or Patient/User Managed Records	Patient/User Read of Self-Submitted Medical Data and Appointments	View previously submitted self (user) request containing medical data. View medical data previously added to a standalone condition management application. View and amend self (user) booked appointments. Viewing of medical data in an online sexual/reproductive health setting.	Low[1]	Strong
	Patient/User Write and Submit Self-Submitted Medical Data,	Submission of user request containing medical data e.g. image. Submit blood pressure readings for review by GP prior to adding to record.	Medium[2]	Strong
	Patient/User Write and Submit Self-Submitted Condition Data or Sexual/Reproductive Health Data.,	Self (user) added medical data to a standalone condition management application. Self (user) added submission of medical data in an online sexual/reproductive health setting.	Low	Basic

	Patient/User Requested Appointment	Book an appointment	Low	Basic
	Patient/User Read of Demographic and Contact Details	View previously user submitted service request to change contact details. View demographic or contact details previously added to.	Low[1]	Strong
	Patient/User Write of Demographic and Contact Details	Submit user request to change contact details.	Medium	Strong
		Add demographic or contact details to a standalone condition management application/	Low	Basic
	Patient/User Write and Submit SelfSubmitted Condition Data or Sexual/Reproductive Health Data.,	Self (user) added medical data to a standalone condition management application. Self (user) added submission of medical data in an online sexual/reproductive health setting.	Low	Basic

[1]Only when using the same authentication credentials as used to add the original data, and only when the data has not been added to or enriched by the service/provider/clinician. Otherwise, High verification is required.

[2]The expectation is that submissions are subject to additional verification checks before clinical decisions are made or official records updated. Otherwise, High is required.

It is up to the service to determine the risk associated with the specific data or transaction being made available.