The NHS Wales Digital Health Identity Standard for Primary Care (NHS Login)

Contents

The NHS Wales Digital Health Identity Standard for Primary Care (NHS Login)

The NHS Wales Digital Health Identity Standard for Primary Care (NHS Login) is based on the established information standard DCB3051, published by NHS Digital (now NHS England). This standard is issued by Welsh Government for use in general practice in Wales.

In the future the use and applicability of this standard may be extended.

Glossary of Terms

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

Authentication - Authentication of a person's identity. Credentials issued and checked on subsequent visits.

Child - A child is defined by the Children's 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 parental 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.

Clinical Staff / Clinicians - A medically qualified health professional registered with a professional body who is directly responsible for the care and treatment of individuals.

Digital health care services - A healthcare service provided by an NHS organisation that is either wholly or partly available digitally.

GDS - The Government Digital Service is part of the Cabinet Office and handles the digital transformation of UK government.

GMS - The main contract framework in the NHS by which most GPs provide care to patients.

GPG44 - See References section below.

GPG45 - See References section below.

Health Professional - A person employed by the organisation for the purpose of delivering NHS services. This includes clinical staff and non-clinical staff with delegated authority to undertake activities that relate to the delivery of healthcare services.

Identity Verification - Verification of identity evidence that may be presented by a person to support proving their identity.

NHS Digital - The former national provider of information, data, and IT systems for commissioners, analysts and clinicians in health and social care in England, particularly those involved with the NHS. NHS Digital's functions were absorbed into NHS England in 2023.

NHS England - The NHS body that oversees the budget, planning, delivery and day-to-day operation of the commissioning side of the National Health Service in England. NHS England also provide information, data, and IT systems for commissioners, analysts and clinicians in health and social care in England, particularly those involved with the NHS.

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.

Registry - Where granted access is recorded and referred to, and the audit trail of who checked and granted the access.

References

The following documents are referenced throughout this document:

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.

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.

GPG44 - Good Practice Guide 44 "Using authenticators to protect an online service" 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.

GPG45 - Good Practice Guide 45 "How to prove and verify someone's identity" is a document by the Cabinet Office that provides guidance on the identity proofing and verification of an individual using online services.

Getting started with records access: Guidance for general practice- Getting started with records access: Guidance for general practice is a document by the RCGP about getting ready for online records access for when patient-facing services become available online.

GP Online Services Guidance: Coercion - GP Online Services Guidance: Coercion 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.

GP Online Service Toolkit - GP Online Service Toolkit is a document by the Royal College of GPs (RCGP) that summarises expert opinion and feedback explaining what online access involves, provides key messages for a number of key stakeholder groups, and outlines future steps to support practices with Patient Online. The Toolkit can be found at: http://www.rcgp.org.uk/patientonline

GP Practice Guidance: Identity Verification for WIVS - GP Practice Guidance: Identity Verification for WIVS is a document produced by Digital Health and Care Wales to help General Practice apply consistent good practice in identity management when providing patients access to online services such as booking appointments, ordering repeat prescriptions, and viewing clinical records.

1 Introduction

What is this standard for?

This standard provides a consistent approach to how a patient can prove their identity when using a service that utilises NHS Login as a means of identification.

Where used by the NHS in Wales, access to NHS Login is provided on behalf of NHS Wales by NHS England. To ensure consistency, this standard is therefore based on DCB3051 - a standard maintained by NHS England. The standard in NHS England was created 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 of effort and to avoid duplication of effort. Elements considered by this standard include:

- identity verification
- identity authentication
- clinical authorisation
- typical example transactions.

This standard will be updated as and when required.

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
- re-verification or re-authentication, although this will be revisited in later versions
- cyber security, threat detection, or other related disciplines.

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

Who does this standard apply to?

This standard applies to GPs in General Practices who deliver identity services for individuals accessing online digital healthcare services in Wales.

What about other available identity standards?

This standard is intended to co-exist with other identity standards such as the UK Cabinet Office good practice guide, GPG45 How to prove and verify someone's identity.

Why is this standard needed?

We want to put people in control of their own healthcare so that they can make informed decisions. We also want to support people such as carers and family members who need to access a person’s healthcare services on their behalf.

Digital healthcare services contain a person's information and will increasingly allow a person to manage their healthcare using digital solutions such as the NHS Wales App. Having an online identity will make it easier and quicker for a person to access online health 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.

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. NHS login offers a facility to enable users to verify their identity online.

For some people, it may not be possible to do this entirely online. This may include situations where individuals do not have the required photo identity documents, or because they have a disability that precludes them from doing so, or because their identity could not be verified by the online service. 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 GP practice.
If a person doesn't have sufficient evidence to verify their identity, it may be possible for a health professional employed in the verifying organisation, who knows the person, to reliably vouch for them and confirm who they are. This may include the person's GP or a practice nurse.

2 Identity in Digital Healthcare

The need for digital identity

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

Healthcare 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 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 healthcare 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.

Healthcare 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 healthcare information obtained fraudulently cannot be recovered and its unauthorised sharing and use cannot be undone.

Since any healthcare information relating to an individual is considered sensitive, information held by healthcare services must only be accessible online by the person to whom it belongs. 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 healthcare 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.

3 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 terms and concepts from GPG45 and the Identity Verification and Authentication Standard for Digital Health and Care Services, DCB3051 Amd 7/2020.

Important principles for identity verification from GPG45 are that:

- 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"

Requirements for identity verification by documentary evidence at a GP Practice

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

1. Two forms of identity, including an item of official photographic identity (such as a passport or driving licence) from the list at Appendix D of this document.
2. Know that the documents appear 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 Welsh Demographic Service (Wales) or the Personal Demographics Service (PDS) (England and Wales).

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).
2. The objective of face-to-face vouching is to reliably link a person to an existing healthcare record under which they are being treated. In many cases this would be supported by the relationship that exists between the patient and the health professional. 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. Vouching is beneficial for people who do not have valid forms of ID, but who may wish to access digital NHS services. This service will only be available for the purpose of providing access to the NHS Login service.
3. Only a health professional who has authorised access to a person's health care record (i.e. they are trusted) can link the record to that person via face-to-face vouching. This precludes other people and professionals (as detailed in Countersigning passport applications and photos) from being able to vouch face-to-face for a person, as they do not have authorised access to the record that requires linking.
4. Face-to-face vouching should be accompanied by appropriate supporting evidence if it is required in the opinion of the health professional carrying out the vouching.
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 GP Practice Guidance: Identity Verification for WIVS

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

Auditing identity verification

The process of identity verification, however implemented, should be audited 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.

GP Practice Guidance: Identity Verification for WIVS provides more guidance on this.

4 Authentication

After having their identity verified, authentication is the technical process for a person to prove who they are each time they access an online health 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:

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.

Strong authentication

Strong authentication requires:
• Multi-factor authentication.
• A mechanism to prevent replay attacks.

Basic authentication

A basic, single factor, form of authentication such as the common approach of using an email address and password.

Please also see "Appendix C – Authentication and verification transactions".

5 Clinical authorisation

Clinical authorisation is a separate concept to authentication which must occur before a person is given access to health records held by a specific service. For example, if a person is granted access to their secondary care record it does not confer the ability to validate for NHS Login. Clinical authorisation is the process used to determine whether an authenticated person is allowed access to a specific digital health care service. For example: their clinical record (and if so, what part of their record).

As a general guide for all services, RCGP guidance for general practice within "GP online services toolkit" lists the following points which must be considered:

- the need to check for and remove any third-party data that wasn't intended to be viewed by the person to whom the record belongs
- records to be checked thoroughly to minimise the risk of patient harm, where necessary including redaction and deferring access until it has been discussed with the patient
- whether the patient is at risk of coercion to share access to online services unwillingly. (see GP Online Services Guidance: Coercion)
- managing access by children or their parents
- patients who lack the mental or physical capacity to use online services themselves
- awareness of the RCGP's Patient Online: The Road Map information governance risk register.

6 Issues and escalation

There must be a defined process for raising issues, such as potential or actual exposure of credentials (username or 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).

Appendices

Appendix A – General principles for identity verification and authentication

The following principles have been identified for this standard:

1. NHS settings

Principle

o NHS identity verification is carried out in conjunction with an NHS patient record o NHS identity may or may not relate to current legal identity.

Rationale

o The online identity created does not exist in isolation to the medical record, it is an online account bound to an existing medical record

o Individuals may have changed their legal name (via deed poll or marriage) without updating the name on their medical record.

Implications

o 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 the health service

Principle

○ Digital identities should be portable across healthcare environments where these utilise NHS login

○ 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 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 or 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 - therefore 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
o 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 – GPG45 element scoring

The objective of the authentication service is to manage specific risks within the context of health care services, not to attain a specific level of assurance in GPG45. In developing The Identity Verification and Authentication Standard for Digital Health and Care Services a common terminology was developed by the former NHS Digital 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.

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

Element A

Purpose: To obtain evidence of the claimed identity ('strength')

Required score: Documentary evidence should (*see section 3) include photo identification (Score 3)

Justification: Identity Evidence is required to support a link to the existing medical record, rather than to create a new identity.

Element B

Purpose: To check the evidence is genuine or valid ('validity'

Required score: 1

Justification: Identity Evidence is required to support a link to the existing medical record, rather than to create a new identity.

Element C

Purpose: Check that the identity belongs to the person who's claiming it ('verification')

Required score: 3

Justification: A physical comparison is required. Biometric comparison would have been possible but there is no biometric database to enable comparison.

Element D

Purpose: Check if the claimed identity is at high risk of identity fraud ('identity fraud')

Required score: n/a

Justification: 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.

Element E

Purpose: Check the claimed identity has existed over time ('activity')

Required score: n/a

Justification: 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 C – 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 transaction archetypes (i.e. typical examples). These archetypes encompass a range of conceptual transactions with some examples being given in the table below that are adopted by NHS Wales for consistency across the NHS.

Transaction type: Patient/User Read Medical Data, Clinical Transactions and Appointments

Verification level: High

Authentication level: Strong

Transaction examples: Read from the GP record; View messages from a clinician; View current and previous appointments booked.

Transaction type: Patient/User Write Medical Data, Clinical Transactions and Appointments

Verification level: High

Authentication level: Strong

Transaction examples: Submit medical readings directly to GP record; Order a repeat prescription; Manage booked appointments.

Transaction type: Patient/User Read of Demographic and Contact Details

Verification level: High

Authentication level: Strong

Transaction examples: Read contact details from the GP record (e.g. address, mobile number).

Transaction type: Patient/User Read of Contact Details

Verification level: High

Authentication level: Strong

Transaction examples: Read contact details from the GP record (e.g. address, mobile number).

For the purposes of the transaction types above, identity verification and authentication is explained as follows:

Purpose: Identity verification
Level: High
Explanation: Identity verification requiring physical comparison in conjunction with sufficient evidence to validate it (refer to appendix B). This is elaborated in Section 3 of this standards document.

Purpose: Identity verification
Level: Medium
Explanation: 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).

Purpose: Identity verification
Level: Low
Explanation: 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 patient's NHS record. If necessary, the relevant medical information should be sent to a clinician for review and that clinician could then add appropriate information to the NHS record following appropriate assessment / verification.

Purpose: Identity authentication
Level: Strong
Explanation: Two-factor authentication as described in Section 4 of this standards document.

Purpose: Identity authentication
Level: Basic
Explanation: User-selected identity and password as described in basic authentication in Section 4 of this standards document.

All organisations should meet the same standards of verification and authentication to ensure portability, though the mechanisms for achieving this may vary between organisations or over time reflecting the evolution of the mechanisms.

Appendix D – Valid identification items for NHS Wales Digital Health Identity Standard for Primary Care (NHS Login)

Score of 2

- A Home Office travel document:
  - convention travel document
  - stateless person's document
  - one-way document
  - certificate of travel
- Other official government or local authority issued travel cards as issued in the UK (for example, a Freedom Pass)
- A marriage or civil partnership certificate
- 60 and Over Welsh Concessionary Travel Card
- Disabled Person's Welsh Concessionary Travel Card
- A firearms certificate
- An education certificate from a regulated and recognised educational institution (such as an NVQ, SQA, GCSE, A level or degree certificate)
- A birth or adoption certificate
- A Blue Badge
- A 'substantial' electronic identity' from a notified eIDAS scheme
- A proof of age card recognised under the Proof of Age Standards Scheme (PASS)
- A gas or electric credit account
- A rental or purchase agreement for a residential property

Score of 3

- Passports that meet the International Civil Aviation Organisation (ICAO) specifications for machine-readable travel documents, such as a South African passport
- Identity cards from an EU or European Economic Area (EEA) country that follow the Council Regulation (EC) No 2252/2004 standards
- UK photocard driving licences
- EU or EEA driving licences that follow the European Directive 2006/126/EC
- UK electoral identification document (for example, a Voter Authority Certificate)
- A US passport card
- A bank, building society or credit union current account (which the claimed identity can show by giving you a bank card)
- A student loan account
- A credit account
- A mortgage account (including buy to let mortgage accounts)
- A digital tachograph driver smart card
- An armed forces identity card
- A proof of age card recognised under PASS with a unique reference number
- A loan account (including hire purchase accounts)
- A 'high' electronic identity from a notified eIDAS scheme

Score of 4

- Biometric passports that meet the ICAO specifications for e-passports, such as a UK passport
- Identity cards from an EU or EEA country that follow the Council Regulation (EC) No 2252/2004 standards and contain biometric information
- A UK biometric residence permit