

Digital Identity Requirements

**Requirements for providers of digital
identity verification services to the NHS**



Contents

Introduction	3
1. Identity in the NHS	4
2. Governance and legal framework	4
2.1 Identity service providers or digital verification service providers	4
Becoming an NHS IDSP	5
3. DVS providers procurement	6
DVS providers procurement	6
Risk assessment	6
Initial presentation of the individual at the relying party	6
4. Digital identity verification requirements	7
4.1 Certification	7
4.2 Outcome of identity verification	7
4.3 Levels of Confidence (LoC)	7
4.4 Identity fraud and mortality checks	7
4.5 Multiple use digital identities (reusability)	8

Introduction

NHS Employers Identity check guidance states:

“An identity check verifies that an individual is who they say they are. It is the most fundamental of all the employment checks.”¹

Digital identity verification is a secure and efficient mechanism for an individual to provide evidence of who they are and satisfy a business or party that requires a valid proof of identity before a transaction can occur. Digital identity verification provides a non-face-to-face alternative to the existing manual approach to identity checks that is employed across NHS trusts.

The UK government has outlined its approach for enabling people to prove their identity digitally through the UK Digital Identity and Attributes Trust Framework (UKDIATF). Consequently, other bodies such as the Disclosure and Barring Service (DBS) have developed their own guidance, outlining how digital identity can be used to verify an individual's identity, as part of an application for a DBS check.

There are digital identity requirements that are specific to the NHS; these are detailed in this document. It outlines the approach that NHS organisations can take to digitally verify an individual's identity in a way that satisfies their obligatory requirements as providers of regulated activities and complies with the UKDIATF.

This document has been designed to complement the existing NHS Employer's identity checks guidance and the UKDIATF in the same way other schemes do. The aim is to enable an individual to obtain a digital identity that can be securely shared with and trusted by multiple NHS trusts, thus facilitating a reduction in burden for organisations and individuals by digitalising the business process of identity verification and reverification.

The digital identity requirements that are specific to the needs of the NHS are contained in this document. NHS trusts should use these requirements when procuring the services of an identity service provider or when verifying identity of their staff to ensure they are compliant with NHS Employers identity checks guidance.

The requirements detailed in this document will evolve to become the NHS Digital Identity Scheme (NDIS) and NHS England along with partners reserve the right to revise the requirements in this publication.

¹ April 2023 - [Identity checks standard | NHS Employers](#)

1. Identity in the NHS

Recruiting staff into NHS positions; including volunteers, temporary workers and contractors must be undertaken in accordance with the [NHS Employment Checks Standards](#). These standards include 6 checks that set out the minimum requirements and allowable variations prior to and during employment. Identity verification forms a fundamental part of all robust employment checks.

To protect the public, it is essential that individuals involved in the provision of healthcare services meet certain requirements and verification of an employee's identity is therefore an obligatory requirement for all NHS employers. The Health and Social Care Act requires NHS organisations to verify the identity of their employees and provide the proof of identity, including a recent photograph to the Care Quality Commission (CQC), if requested.

The April 2022 legislation that allows UK certified Identity Service Providers to use Identification Document Validation Technology (IDVT) for pre-employment and criminal record checks does not absolve NHS trusts from their identity checking obligations, as a provider of regulated activities. Therefore, due care and considerations must be given when digital identity is being considered within the recruitment process of an NHS trust. This document sets out the key requirements for digital identity in the NHS.

2. Governance and legal framework

This requirement document sets out how NHS trusts can meet their obligations to verify the identity of both prospective and existing NHS employees, as defined in the *NHS Employer's identity checks guidance*². For digital identity verification, these obligations can be met by using certified identity service providers (Certified IDSPs) or in the future, a certified digital verification service (DVS) provider.

A Relying Party such as an NHS trust who is consuming and trusting the services of the certified DVS provider will not need to undertake additional due diligence on the verified digital identity if the identity has been verified by a Certified DVS provider and the requirements detailed in this document are met. For example, the Level of confidence (LoC) must meet the required level, as specified in section 4.2 below.

2.1 Identity service providers or digital verification service providers

A list of certified DVS providers, the schemes against which they are certified and certificates showing the levels of confidence the DVS providers can meet is published by the Department for Science, Innovation and Technology (DSIT)³. This requirement document makes reference

² April 2023 - [Identity checks standard | NHS Employers](#)

³ [Digital identity certification for right to work, right to rent and criminal record checks - GOV.UK \(www.gov.uk\)](#)

to and aligns with the DSIT UK digital identity and attributes trust framework⁴ (UKDIATF) which:

- defines the organisational responsibilities that DVS providers must meet, in order to be certified by a certification body which has been accredited by the UK Accreditation Service (UKAS) against the UKDIATF.
- requires that once certified, DVS providers must undertake annual surveillance audits and biennial recertification by a government certification body against the most recent version of the UKDIATF available at the time.
- references the UK Government Good Practice Guide 45⁵ (GPG45) as the standard that is used to define how identities should be verified using 'Levels of Confidence (LoC)' and 'identity profiles' that can meet the levels of confidence.

NHS IDSPs will be required to be either:

1. IDSPs⁶ or DVS providers procured via a procurement call off that includes a legal obligation to meet the additional requirements as defined in section 4 of this document.

Or

2. IDSPs⁷ or DVS providers certified by a UKAS-accredited certification body against the requirements set out in the UKDIATF **and** the NHS Digital Identity Scheme when it becomes available.

Becoming an NHS IDSP

The NHS digital identity scheme will undergo a process of authorisation and publication by DSIT along with other schemes. Following this, certified IDSPs or DVS providers will be able to get themselves certified against the NHS Digital Identity scheme and NHS trusts will have option 2 above, available to them.

For now, only option 1 above is the currently available route for NHS IDSPs.

⁴ [UK digital identity and attributes trust framework beta version \(0.3\) - GOV.UK \(www.gov.uk\)](#)

⁵ [How to prove and verify someone's identity - GOV.UK \(www.gov.uk\)](#)

⁶ IDSPs identified via the DSIT trusted list

⁷ IDSPs identified via the DSIT trusted list

3. DVS providers procurement

DVS providers procurement

NHS trusts should ensure the requirements in section 4 below are placed on their IDSPs when selecting or procuring their services. This will ensure important sets of information that are required for establishing employee identity and enabling recruitment decision-making are fully considered from the onset of their engagement with IDSPs. IDSPs will collect, verify and make all the required information available to the employing organisation, including

- personal identification information of the individual
- details of evidence reviewed to complete the identity verification
- a verified high-resolution photograph of the individual
- the GPG45 LoC reached

Risk assessment

This requirement document does not replace the NHS trust's responsibility to carry out a risk assessment for every transaction. The NHS trust's remains liable for undertaking their own due diligence of which the identity verification process forms a part of the risk assessment.

NHS IDSPs simplify the risk assessment process by allowing an NHS trust to rely on a verified identity from an NHS IDSP as having met a required level of confidence.

NHS IDSPs undertake their own risk assessment during the identity verification process in order to provide a verified identity at the LoC required by the NHS trust. NHS trusts do not need to undertake additional due diligence on the NHS IDSP or the verified identity if the identity has been verified by a Certified IDSP and the requirements detailed in this document are met.

NHS trusts must retain evidence of employee identity verification such as the identity verification report, in accordance with their trust's retention policy for personal records, just as they would for non-digital identity verifications.

Initial presentation of the individual at the relying party

The Relying Party or the NHS trust consuming the services of a DVS provider must satisfy themselves that the high-resolution photograph and biographic details are consistent with the individual presenting themselves for work i.e., the information provided by the digital identity check relates to the individual and they are not an imposter. For example, the NHS trust would perform a check to compare the individual employee with a verified high-resolution image supplied by the NHS IDSP to ensure it is of the same person.

4. Digital identity verification requirements

DVS providers providing identity verification services to NHS organisations must meet the following set of requirements.

4.1 Certification

NHS DVS providers must be certified to complete **reusable** identity verifications, Right to Work (RTW) checks and Enhanced with Barred Lists DBS eligibility checks on behalf of employers. NHS DVS providers must also be certified against the most current version of the UKDIATF available at the commencement of their certification journey.

4.2 Outcome of identity verification

NHS DVS providers must return a range of attributes that provide details of the process and the outcome of the identity, RTW and DBS eligibility checks of an individual to enable a Relying Party such as an NHS trust make appropriate decisions. These attributes must include as a minimum, the digital identity attributes specified for an individual as per the DSIT trust framework data schema. In addition, the RTW evidence check credential attributes and supplementary attributes required to complete a DBS check must be included where they are available. Attributes should be provided as distinct credentials to enable the reuse of credentials. Details of additional attributes are specified in the NHS Technical Trust Framework for Verifiable Credentials Data Schema⁸.

NHS trusts must retain the outcome of all verifications received from DVS providers in accordance with their retention policy for employee pre-employment records.

4.3 Levels of Confidence (LoC)

Verifying an individual's identity against GPG45 requires NHS IDSPs to follow a five-part process known as 'identity checking', where each step of the process is scored, and used to determine which of GPG45's four LoCs (Low, Medium, High, Very High) has been achieved.

The minimum LoC required for NHS staff is **High**.

4.4 Identity fraud and mortality checks

Identity fraud, evidence and mortality checks must be undertaken on the claimed identity, during the initial identity verification and proofing checks. The DVS provider is expected to

⁸ [NHS Technical Trust Framework for Verifiable Credentials Data Schema](#)

complete further periodic checks on the claimed identity. The minimum periodic check expected is at 180 days after the initial identity verification was completed.

4.5 Multiple use digital identities (reusability)

To enable staff movement within the NHS, verifiable credentials such as digital identity, training and vaccination records are to be issued into an NHS approved digital wallet (currently Microsoft Authenticator) which will interoperate with the NHS digital staff passport solution. Reusability of credentials, including identity and RTW evidence check credential is an important NHS requirement. Therefore, NHS DVS providers must:

- make the digital identity check available as a W3C verifiable credential (VC) and issue the verifiable credential into an NHS approved digital wallet; this is currently the Microsoft authenticator wallet.
- ensure that where individual VCs need to be revoked or suspended the relevant entries are maintained in a Status List service.
- ensure that for each VC, the issuer of the VC is a member of the NHS digital identity verification register so that the NHS can check the DVS provider is not suspended as an issuer, be it at the point of the initial sharing of the credential or subsequently.
- adopt the NHS Identity schema defined in the NHS Technical Trust Framework that describes attributes to be included when a W3C verifiable credential (VC) is issued.
- protect reusable digital identities by meeting the requirements and following the guidance on using authenticators to protect an online service, also known as GPG44 as specified in 13.1 in the UKDIATF.
- make available the high-resolution photograph of the individual that was taken, by the individual (a selfie), during the identity verification process and successfully matched to the reference image held on the strongest piece of evidence presented by the individual. The metadata should describe, when the photo was taken, the evidence type it was compared with and the NHS DVS provider that performed the successful match.
- Ensure digital identities are valid for multiple use as per terms to be agreed.