

# Identity Verification and Authentication Standard for Digital Health and Care Services

Version 1.0

21st June 2018

**Information and technology**  
**for better health and care**

# Data Coordination Board

This information standard (DCB3051) has been approved for publication by the Department of Health and Social Care under [section 250 of the Health and Social Care Act 2012](#).

Assurance that this information standard meets the requirements of the Act and is appropriate for the use specified in the specification document has been provided by the Data Coordination Board (DCB), a sub-group of the Digital Delivery Board.

This information standard comprises the following documents:

- Specification incorporating implementation guidance.

An Information Standards Notice (DCB3051 Amd 64/2018) has been issued as a notification of use and implementation timescales. Please read this alongside the documents for the standard.

The controlled versions of these documents can be found on the [NHS Digital website](#). Any copies 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.

Date of publication: 29 June 2018

# Contents

|  |           |
|--|-----------|
| Glossary of Terms  | 4         |
| References   | 5         |
| <b>1 Introduction</b>  | <b>6</b>  |
| What is this standard for?   | 6         |
| What is not covered by this standard?  | 6         |
| Who does this standard apply to?   | 6         |
| What about other available identity standards?                               | 6         |
| Why is this standard needed?   | 7         |
| What is required?  | 7         |
| <b>2 Identity in Digital Health and Care</b>                                 | <b>8</b>  |
| The need for digital identity  | 8         |
| Overview of identity verification and authentication                         | 9         |
| <b>3 Identity verification</b>   | <b>9</b>  |
| Requirements for identity verification                                       | 10        |
| Face-to-face vouching  | 10        |
| Auditing identity verification   | 11        |
| <b>4 Authentication</b>  | <b>11</b> |
| Strong authentication  | 11        |
| Basic authentication   | 11        |
| <b>5 Clinical authorisation</b>  | <b>12</b> |
| <b>6 Delegated access</b>  | <b>12</b> |
| <b>7 Issues and escalation</b>   | <b>13</b> |
| <b>8 Appendices</b>  | <b>14</b> |
| Appendix A – General principles for identity verification and authentication | 14        |
| Appendix B – PCAG Privacy Principles   | 16        |
| Appendix C – GPG45 element scoring   | 17        |
| Appendix D – Authentication and verification transactions                    | 18        |

## Glossary of Terms

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

| Term or Abbreviation                             | Definition and further information  |
|--|---|
| <a href="#">Health and care organisation</a>     | Any NHS or non-NHS provider, organisation, company, or authority offering health and care services including social care.   |
| <a href="#">Digital health and care services</a> | 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.  |
| <a href="#">Delegated access</a>                 | Also referred to as proxy access.<br>The sharing of a person's access to health and care services with a nominated other person, referred to as a proxy. For example: parent-child relationships, and family members acting as a carer. |
| <a href="#">Identity Verification</a>            | Verification of identity evidence that may be presented by a person to support proving their identity.  |
| <a href="#">Physical Comparison</a>              | 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.   |
| <a href="#">Authentication</a>                   | Authentication of a person's identity. Credentials issued and checked on subsequent visits.   |
| <a href="#">Clinical Authorisation</a>           | 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.                             |
| <a href="#">Registry</a>                         | Where granted access is recorded and referred to, and the audit trail of who checked and granted the access.  |
| <a href="#">GPG44</a>                            | See References section below.   |
| <a href="#">GPG45</a>                            | See References section below.   |
| <a href="#">GDS</a>                              | The <a href="#">Government Digital Service</a> is part of the Cabinet Office and handles the digital transformation of government.  |
| <a href="#">NHS Digital</a>                      | The 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.   |
| <a href="#">PCAG</a>                             | The <a href="#">Privacy and Consumer Advisory Group</a> advises the government on how to provide users with a simple, trusted and secure means of accessing public services.  |
| <a href="#">DCB</a>                              | The Data Coordination Board is a national body that approves the publication of standards for use across health and social care.  |

## References

The following documents are referenced throughout this document:

| Ref. No. | Document Title<br>(click for link)  | Further information<br>(click blue document titles for links)  |
|----------|---|--|
| 1        | <a href="#">GPG45</a>   | <a href="#">Good Practice Guide 45</a> "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        | <a href="#">GPG44</a>   | <a href="#">Good Practice Guide 44</a> "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.   |
| 3        | <a href="#">GPG43</a>   | <a href="#">Good Practice Guide 43</a> "Requirements for Secure Delivery of Online Public Services", which sets out an approach to determining the necessary components to deliver public services securely online.  |
| 4        | <a href="#">Patient Online: The Road Map</a>  | <a href="#">Patient Online: The Road Map</a> is a document by the Royal College of GPs 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.   |
| 5        | <a href="#">Good Practice Guidance on Identity Verification for Patient Online Services in Primary Care</a> | <a href="#">Good Practice Guidance on Identity Verification for Patient Online Services in Primary Care</a> is a document by NHS England 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. |
| 6        | <a href="#">Getting started with records access: Guidance for general practice</a>                          | <a href="#">Getting started with records access: Guidance for general practice</a> is a document by the RCGP about getting ready for online records access for when patient-facing services become available online.   |
| 7        | <a href="#">Coercion: Guidance for general practice</a>   | <a href="#">Coercion: Guidance for general practice</a> 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.   |
| 8        | <a href="#">Countersigning passport applications and photos</a>   | <a href="#">Countersigning passport applications and photos</a> is a GOV.UK online guide to the countersigning requirements for passport applications and photos.  |

# 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 Digital has worked on this standard in conjunction with many key clinical and privacy stakeholders including NHS England, 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. The national Data Coordination Board (DCB) will approve the publication of all versions.

Feedback on this standard is welcome at any time. Comments can be sent to [cid.phr@nhs.net](mailto:cid.phr@nhs.net).

## 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 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 alone. See also [GPG43 "Requirements for Secure Delivery of Online Public Services"](#)<sup>3</sup>.

## Who does this standard apply to?

Any NHS or non-NHS provider, organisation, company, or authority that provides identity services for individuals accessing online digital health or care services must adhere to this standard.

## What about other available identity standards?

This standard is intended to co-exist with other identity standards such as [GPG45 "Identity proofing and verification of an individual"](#)<sup>1</sup>.

## 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, heartrate 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.



## 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 GP practice, or a Post Office.

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.

## 2 Identity in Digital Health and Care

### 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 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.



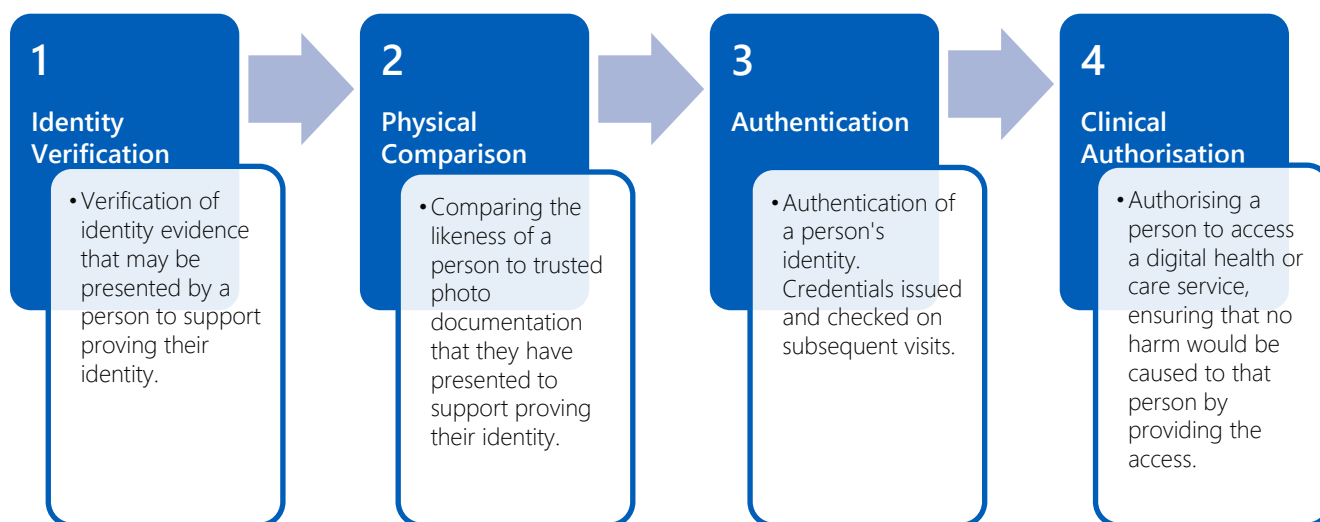
Delivering services online has significant implications for how we deliver health and care services in future. Controls that are typically built implicitly into the healthcare process (e.g. via a GP consultation) such as trust, privacy, clinical safety and security now need to be delivered digitally.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

## 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:



## 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<sup>1</sup>](#).

Important principles for identity verification from Chapter 3 in [GPG45<sup>1</sup>](#) 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<sup>1</sup>](#) 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) from the list in Table 14 in [Annex A of GPG 45<sup>1</sup>](#).
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. If the photographic identity does not include address details, then a further non-photographic piece of Identity Evidence is required. This must include the name and address and be reasonably expected to have been delivered to that address.
5. The individual is not deceased, by reference to an Authoritative Source such as the [Personal Demographics Service \(PDS\)](#).

## 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<sup>8</sup>](#)).
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 care worker would be vouching for the fact that the record under which they are caring for a person relates to that person. A GP would be vouching for the fact that the practice record under which they are treating a person relates to that person.
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 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<sup>8</sup>](#)) 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 or care professional carrying out the vouching.
5. Where necessary the vouching can be supported with clinical questions against the record – see [NHS England Good Practice Guidance on Identity Verification for Patient Online Services in Primary Care<sup>5</sup>](#).

Please also see “[Appendix C – 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.

## 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 or care service.

This usually means 'logging on' to a system with a username and password. Sometimes an additional step is required, known as two-factor authentication (2FA), such as entering a code sent in a text message to the person's mobile phone.

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

1. **something you have** - such as a code sent in a text message to a mobile phone
2. **something you know** - such as a password, passphrase, or memorable information
3. **something you are** - such as a fingerprint, iris scan, or facial recognition (i.e. biometrics)

A digital health or care service can be accessed using one of two types of authentication, depending on various factors such as the sensitivity of the service and the information that can be accessed and/or recorded. See "Why is this standard needed?" in Section 1. An online health or care service must choose the authentication method that best suits its security and access requirements.

### Strong authentication

Standard LOA 2 authentication from [GPG44<sup>2</sup>](#) to prevent replay attacks and to ensure access is by the authenticated individual. This is summarised as using:

- two-factor authentication (as described above)
- a mechanism to prevent replay attacks.

### Basic authentication

A basic form of authentication such as the usual approach of using a username and password. This may be deemed adequate for services such as booking GP appointments.

Please also see "[Appendix D – Authentication and verification transactions](#)".

## 5 Clinical authorisation

Clinical authorisation is a separate concept to authentication which must occur when a person requests or is given access to a record held by a specific service. For example, if a person is granted access to their hospital care record it does not give automatic access to other records such as those held by their GP or community nurse; each service must follow its own process for authorising people to access the record which they have responsibility for. Clinical authorisation is the process used to determine whether an authenticated person is allowed access to a specific digital health or care service. For example: their clinical record (and if so, what part of their record). If clinical authorisation is not required to access a particular online health and care service, then access should be allowed by default.

RCGP guidance for general practice about “[Getting started with records access](#)”<sup>6</sup> 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
- whether the patient is at risk of coercion to share access to online services unwillingly. (see [Coercion: Guidance for general practice](#)<sup>7</sup>)
- 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](#)<sup>4</sup> information governance risk register.

## 6 Delegated access

It is important for a person to be able to share their access to certain online health and care services with other nominated people. This is known as delegated access and is also sometimes referred to as proxy access. It can be necessary where, for example, someone with parental responsibility needs access on behalf of a child, or where a family member needs access on behalf of an elderly relative. The person still retains access to the digital health and care services themselves and they can also determine which digital health and care service(s) each nominated person has access to.

For digital health and care services that provide delegated access, all people involved must go through the identity verification process in this standard. There must be a robust mechanism for recording that delegated access has been granted; the person granting it, the person to whom it was granted, and which digital health or care service(s) it applied to. There must also be a mechanism in place to enable appropriate withdrawal of delegated access, either with or without the consent of the person who has the access.

## 7 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).

## 8 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 carried out in conjunction with an 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**
  - Citizen identity 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 - however 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 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
  - 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 | <b>USER CONTROL</b> "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 | <b>TRANSPARENCY</b> "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 | <b>MULTIPLICITY</b> "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 | <b>DATA MINIMISATION</b> "My interactions only use the minimum data necessary to meet my needs."   | Met. Identity information only held where necessary.   |
| 5 | <b>DATA QUALITY</b> "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 | <b>SERVICE USER ACCESS AND PORTABILITY</b> "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 | <b>CERTIFICATION</b> "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 | <b>DISPUTE RESOLUTION</b> "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 | <b>EXCEPTIONAL CIRCUMSTANCES</b> "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 element 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<sup>1</sup>](#). However, NHS Digital 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<sup>1</sup>](#).

The following table identifies the agreed standard of evidence needed for each element of identity verification as per [GPG45<sup>1</sup>](#).

| Element  | The purpose of this element  | Required score | Justification  |
|----------|--|----------------|--|
| <b>A</b> | To record the strength of the Identity Evidence provided by the Applicant in support of the claimed identity.        | 1              | Identity Evidence is required to support the existing medical record, rather than to create a new identity.  |
| <b>B</b> | To record the score obtained from the Identity Evidence validation process.  | 1              | Identity Evidence is required to support the existing medical record, rather than to create a new identity.  |
| <b>C</b> | To record the score obtained from the identity verification process.   | 3              | A physical comparison is required. Biometric comparison would have been possible but there is no biometric database to enable comparison.  |
| <b>D</b> | To record the score obtained from the identity counter-fraud check process.  | 1              | 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. |
| <b>E</b> | To prove a continuous existence of the Claimed Identity over a period of time backwards from the point of Assessment | 1              | 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 transaction archetypes (i.e. typical examples). These archetypes encompass a range of conceptual transactions with some examples being given in the table below.

For the purposes of the archetype table, identity verification and authentication is explained as follows:

| Purpose                 | Level  | Explanation   |
|-------------------------|--------|---|
| Identity verification   | High   | Identity verification requiring physical comparison (Element C score 3) in conjunction with sufficient evidence to validate it (elements A, B, D, and E score 1). 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 authentication | High   | Two-factor authentication as described in Section 4 of this standards document.   |
| Identity authentication | Low    | 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 (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).

| Arche-type | Category | Archetype Transaction           | Verif-ication | Authent-ication | Transaction examples   |
|------------|----------|---------------------------------|---------------|-----------------|--|
| A1         | Enquiry  | Enquiry against official record | High          | High            | <ul style="list-style-type: none"> <li>• Read medical record, Prescription repeat,</li> <li>• View SCR or detailed record,</li> <li>• Manage / view appointments,</li> <li>• Tailored online NHS services and online content.</li> </ul> |

|    |         |  |        |      |   |
|----|---------|--|--------|------|---|
| A2 | Add     | Record non-medical data outside the patient record     | None   | Low  | <ul style="list-style-type: none"> <li>Book appointment (not able to view or manage appointments – which may give out information)</li> </ul>   |
| A3 | Add     | Record non-medical data into record                    | Medium | High | <ul style="list-style-type: none"> <li>Record data-sharing opt-out preference,</li> <li>Record preferred pharmacy (further controls will be needed around collection of controlled medications).</li> </ul> |
| A4 | Add     | Record medical data into record                        | High   | High | <ul style="list-style-type: none"> <li>Private healthcare consultation record.</li> </ul>   |
| A5 | Add     | Record authorised delegates                            | High   | High | <ul style="list-style-type: none"> <li>Enable delegated access for another validated individual</li> </ul>  |
| A6 | Add     | Record patient registration information                | High   | High | <ul style="list-style-type: none"> <li>Register for online account,</li> <li>Record new phone number online,</li> <li>Record new patient address online</li> </ul>  |
| A7 | Add     | Change GP Practice                                     | High   | High | <ul style="list-style-type: none"> <li>Register patient to a new GP through a purely online mechanism</li> </ul>  |
| A8 | Enquiry | Enquiry of non-medical data outside the patient record | None   | Low  | <ul style="list-style-type: none"> <li>Access non-tailored online NHS services and content.</li> </ul>  |