QIPP Digital Technology

Patient Identity Assurance – Guidance for Patient Portals

Author: Adam Cooper

Date: 23rd March, 2012
Version: 1.0

Amendment History:

Version	Date	Amendment History
1.0		Final version for publication

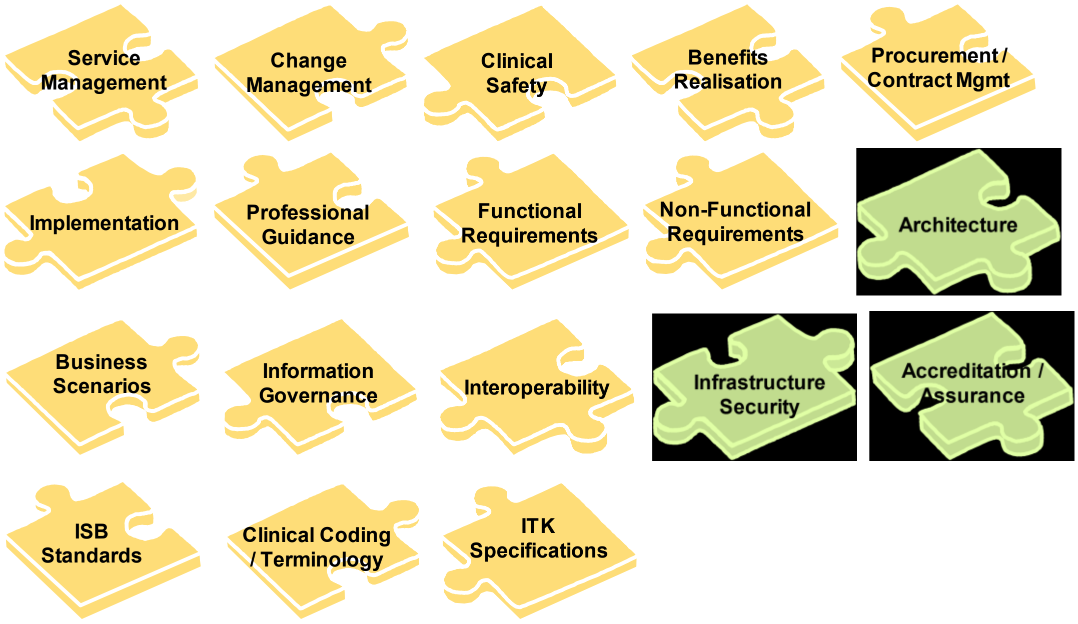
Contents

1. Purpose

This document provides an explanation of the need for patient identity assurance, the risks involved if not assuring identity, and guidance for securely registering and authenticating patients with online health services. This document also provides recommendations for the key steps to be taken and candidate components that would be required for identity assurance.

1.1. Scope

For any technology solution to be implemented within a healthcare setting, a wide range of areas need to be considered. This document is not intended to cover every aspect of the delivery of a solution. The below diagram gives a general overview of some of the areas you may need to consider – the areas that are addressed (at least in part) in this document are shown in green:



1.1.1. Out of Scope

The following are out of scope:

- Recommendations for a specific solution for Patient Identity Assurance
- The functionality or services accessed via portals once a user is authenticated (e.g. maintaining personal health records).

Examples and references may be made to potential future architecture options, such as the Cabinet Office IDA Programme, however these are provided for information only.

1.2. Intended Audience

This document has been written for the QIPP Digital Team to support the development of LTC Portals although it is relevant to anyone wishing to provide Digital Patient services that require patient registration and authentication.

1.3. Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by NHS Connecting for Health. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

Any party relying on or using any information contained in this document and/or relying on or using any system implemented based upon information contained in this document should do so only after performing a risk assessment. A correctly completed risk assessment enables an NHS organisation to demonstrate that a methodical process has been undertaken which can adequately describe the rationale behind any decisions made. Risk assessments should include the potential impact to live services of implementing changes.

This means that changes implemented following this guidance are done so at the implementers' risk. Misuse or inappropriate use of this information can only be the responsibility of the implementer.

2. Background

Quality, Innovation, Productivity and Prevention[1] (QIPP) is a large scale transformational programme within the NHS, involving all NHS staff, clinicians, patients and the voluntary sector. It will improve the quality of care the NHS delivers whilst making up to £20billion of efficiency savings by 2014-15, which will be reinvested in frontline care.

At a regional and local level Strategic Health Authorities have been developing integrated QIPP plans that are supported by national QIPP workstreams which are producing tools and programmes to help local change leaders in successful implementation.

2.1. Specific Workstream Drivers

Through an Expression of Interest process across the QIPP LTC workstream, the need for robust identity assurance during patient registration and authentication to LTC portals has been identified. As a result this guidance document was requested to assist LTC portal developers when considering patient identity assurance.

2.2. QIPP Digital Technology Team

QIPP Digital Technology has been established as a function under the QIPP programme to assist QIPP national workstreams and local teams in exploiting digital technology in order to accelerate delivery of their QIPP priorities[2].

The function focuses on helping to overcome digital challenges and barriers, to accelerate delivery, to spread initiatives and to maximise the potential value from technology enabled healthcare delivery.

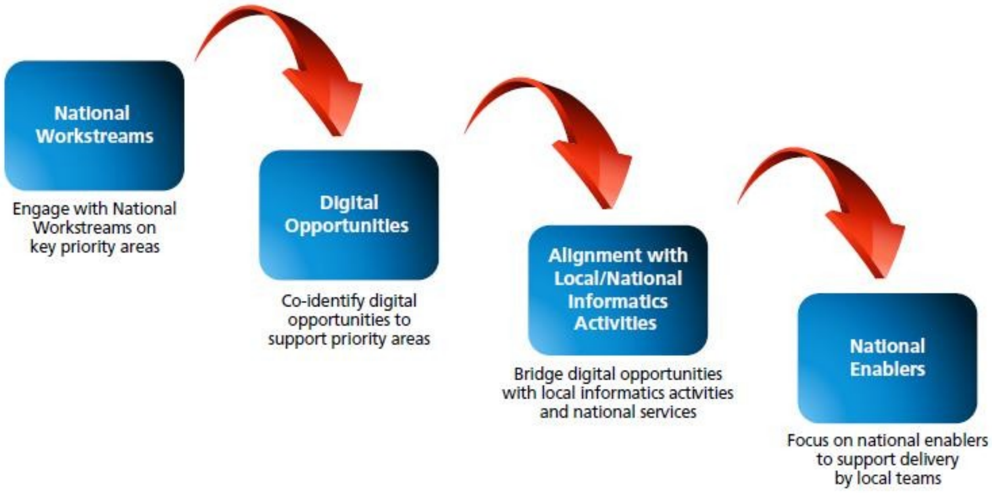

National Workstreams
Engage with National Workstreams on key priority areas
Digital Opportunities
Co-identify digital opportunities to support priority areas
Alignment with Local/National Informatics Activities
Bridge digital opportunities with local informatics activities and national services
National Enablers
Focus on national enablers to support delivery by local teams

Fig. 2.2.1 - QIPP Digital Team Approach

A core principle of this operating model is to ensure that any work conducted or national enablers provided, have direct traceability back to key business drivers, and that work is only undertaken where there is a local 'pull' for national assistance.

[1] DH: QIPP Page - http://www.dh.gov.uk/en/Healthcare/Qualityandproductivity/QIPP/index.htm

[2] NHS Networks: QIPP Digital Technology and Vision - http://www.networks.nhs.uk/nhs-networks/qipp-digital-technology-and-vision

3. Glossary

Term	Description
CESG	Communications-Electronics Security Group – the UK Government's National Technical Authority for Information Assurance
eGIF	e-Government Interoperability Framework
IDA	Cabinet Office cross-government Identity Assurance Programme
LTC	Long Term Condition
PDS	Patient Demographic Service
PAF	Post Office Address File
Personal Health Record	A health record held and maintained by the subject of care or a representative of the subject of care. This is not a centrally held NHS health record.
RSDOPS	Requirements for Secure Delivery of Online Public Services
SAML	Security Assertion Mark-up Language – an XML-based open standard for exchanging authentication and authorization data between security domains.
SSL	Secure Sockets Layer – as used to secure communications between a web browser and an online service
User Agent	A web browser or mobile device accessing an online service.

4. The need for Patient Identity Assurance

Digital channels (the internet, mobile, kiosk, digital TV et al) have the opportunity to bring benefits to all parts of society. However, the convenience of digital channels is countered by a different set of risks and potential for fraud or misuse of personal data.

There is a clear need to provide safe, secure access to healthcare portals and web based applications such as those for Long Term Conditions where patients need regular access to their records (or to contribute to those records) without the need for a clinician to be present. In order to make this a reality it is essential that a robust registration process, including trusted identity verification, coupled with appropriate authentication credentials is put in place.

Evidence for the importance of identity assurance has been noted by other health care organisations and groups such as the Royal College of General Practitioners.

To quote the Royal College of General Practitioners in their document "Enabling Patients to Access Electronic Health Records – Guidance for Health Professionals"[3]:

> *Health organisations should strive to provide a secure mechanism enabling direct Record Access by patients and, when available, inform patients of the facility and how to use it.*

The Royal College goes on to state that:

> *It is essential that the correct patient has access to the correct record. Robust assurance of identity is a prerequisite to registration for a Record Access service.*

Identity is a fundamental principle that underpins the delivery of online transactional services be it Healthcare, online banking services, or retail services. The Government is moving towards public services that are increasingly delivered online increasing the need to build an identity trust framework that enables rather than disables 'digital by default'. From a Healthcare perspective delivering digital online services is driven from the need to provide wider, more convenient access to patient services and records particularly where there is a need for frequent interaction between patients and clinicians.

To mitigate the risks associated with transacting online, almost all services require the user to go through some form of initial registration and subsequent login procedure. These procedures, if not designed correctly, can deter the use and uptake of digital services. Furthermore, fraudsters are developing increasingly sophisticated ways to get around the security procedures.

[3] Enabling Patients to Access Electronic Health Records (Guidance for Health Professionals): Version 1.0 – September 2010 [Brian Fisher, Richard Fitton, Amir Hannan] - http://www.connectingforhealth.nhs.uk/engagement/public/projects/rcgp

The customer (e.g. a patient) generally receives the fall out: security procedures place an increasing burden of responsibility on the customer to remember passwords, carry tokens, update software and ensure that nothing is revealed to an imposter.

A segment of society has become 'digitally disenfranchised': unable or unwilling to engage in the digitally economy and therefore unable to attain the benefits.

The Cabinet Office has defined a strategic approach to Identity Assurance for access to UK Government online services as part of the Digital by Default initiative. Cabinet Office's IDA Programme is an Identity Assurance programme dedicated to the provision of a pan-government system for secure access to government services online, which:

- Provides citizens with a safe and secure means of registering their Identity for use with multiple digital services
- Provides government with a trusted means of authenticating these citizens when using a digital identity with a government service provider (e.g. an LTC Portal)
- Ensures that registration information (how the identity is proved) is neither duplicated or shared (with digital services)

Further details regarding the Identity Assurance Programme may be found in Appendix A.

4.1. Basic principles

The following basic principles should be observed when determining the identity assurance (registration, verification, and authentication) requirements for patient portals such as an LTC portal.

4.1.1. All patient portals should be IG and Risk assessed

Regardless of functionality it is recommended that all patient facing portals undergo a local IG and security risk assessment before implementation. These risk assessments should then be refreshed at regular intervals (e.g. annually) to ensure that identity assurance for portals and the functionality they provide remains appropriate.

4.1.2. User journey affects required identity assurance level

The type of functionality or data accessed by a portal should also be considered during risk assessment as this may directly affect the identity assurance level required.

Type of Portal / Website	Risk Profile
Personal Health Records [4]/ Information Based Site	Low risk. Self asserted / user recorded information such as lifestyle data, basic observations (blood pressure, heart rate etc.). This type of information is of low risk although adequate protection of data for privacy and reputational risk should be considered during risk assessment.
Patient Health Records Access (single patient only)	Medium to High risk. Depending on the characteristics of the service portals of this type may not require eGIF L3 identity assurance although an IG and risk assessment will be required.
Patient Health Records Access (clinician access to multiple patients' records)	High risk. Where multiple clinical/patient records are available to registered users (e.g. clinicians) a high level of assurance will be required to prevent fraudulent or inappropriate access to information.

4.2. Relevant polices and guidance

The need to ensure the confidentiality of (clinical) sensitive data in the NHS has been long recognised. The e-Government Interoperability Framework (e-GIF) was formally adopted by the NHS Technical Standards sub-board on 23 November 2000, and relevant e-GIF standards are included in the NHS IM&T Standards Handbook. This followed a public commitment by the Minister of Health that the NHS would adhere to the standards set out in the e-Government Strategy also published that year. e-GIF is also used as part of the mandatory employment check standards published by NHS Employers.

Subsequently in September 2002, the Office of the e-Envoy published version 3 of the e-Government Strategy Framework Policy and Guidelines for Registration and Authentication as part of e-GIF. This document is now established as part of the e-Government Security Policy Framework, and has not been formally superseded since its issue date.

This was adopted by the Department of Health as directly applicable in defining those security requirements related to the provision of NHS user registration and authentication services. As such procurement or implementation of any services that protect sensitive data in the NHS should provide user registration and Authentication services meeting requirements of e-GIF.

[4] Personal Health Record: a health record held and maintained by the subject of care or a representative of the subject of care. This is not a centrally held NHS health record.

4.2.1. eGIF 2002

The eGIF standard describes the appropriate security requirements related to the provision of registration and authentication services to support access to e-Government services. DHID has adopted this standard for all online service either public or clinician facing. Described within eGIF are a number of Registration and Authentication Levels (L0 to L3) which match the risk assessed for an online service. As eGIF righty states: *"as a rule, service provision should operate on a principle of maximum anonymity consistent with necessary functionality."*

4.2.2. Requirements for Secure Delivery of Online Public Services (RSDOPS)

The Cabinet Office and other government departments such as HMRC and DWP are currently basing their identity assurance assessments on the CESG draft of RSDOPS. This document is not yet an authorised standard for NHS systems but should be referenced if the cross-government IDA Programme is being considered as a potential identity assurance option for your patient portal.

At the time of writing RSDOPS remains in draft form and has yet to be adopted as a DHID standard it is referenced here as a guide for early adopters of services such as the pan-government Identity Assurance model championed by the Cabinet Office.

4.3. Identifying the level of identity assurance required

Each service must assess the type of information stored, the transactions available to users and the risk posed by granting access to this data and functionality online, both to individuals (i.e. patients) and to the service itself. ***In general this can be simplified to two key types of online service in a health setting:***

- services providing access to patient identifiable data and/or patient medical records, and;
- services that do not hold sensitive patient data i.e. medical records (or provide access to such data).

Services that only provide access to information asserted by the user (patient) such as lifestyle information, basic observations (e.g. blood pressure, heart rate etc) pose a much lower risk to privacy or fraudulent attack than those offering access to patient records or other private information such as private correspondence between patients and clinicians, appointment management, or prescriptions.

Functionality of the service should also be considered when determining the level of identity assurance required. Portals that provide access to a single patient record (i.e. the patient registered can see only their own records) pose a much lower risk than services that expose the records of multiple patients to one or more clinicians or other registered users.

4.3.1. Recommended levels for registration and authentication

The eGIF 2002 standard provides a description of service characteristics at each level of registration and authentication and should be cross-referenced following risk and IG assessments of the proposed patient portal to ensure that appropriate levels of assurance for each function are selected.

In general, any service providing access to patient sensitive data (e.g. records) is recommended to implement registration and authentication regimes at level 2 as a minimum based on eGIF 2002 or RSDOPS. It should be noted that this is dependent on risk and IG assessment: each service/application should be assessed separately.

Note, that further detail regarding requirements for registration such as evidence required can be referenced in the full eGIF 2002 documentation.

These registration and authentication levels are summarised below.

Level	Registration Level Description	Authentication Level Description	Service Example
0	***Transactions in which minimal damage might arise from misappropriation of real-world identity.***	No explicit authentication required. Untested session context (e.g. cookies) may be set.	Typically applicable to information-only services where nothing is known, or expected to be known, about the users e.g. website offering public information to individuals e.g. a local NHS Trust website.
1	***Transactions in which minor damage might arise from misappropriation of real-world identity.*** ***Appropriate where the user needs to create an account to build up, and return to, stored information but no association with a real identity is needed, or offered.***	Applicable to public sector services where user authorisation is mandated but strong anti-replay measures are not justifiable. The user will typically be required to expose an authentication secret that was agreed at authorisation e.g. password.	Services which perform simple purchase transactions (e.g. licensing), or those requiring simple registration and user customisation (e.g. NHS Choices for customised content delivery, or online training where progress should be tracked).

2	***Transactions in which significant damage might arise from misappropriation of real-world identity*** ***Appropriate in circumstances where the service needs to collect and collate information on real individuals.*** Potential users will need to present evidence that supports their identity claim including documentary evidence.	The user is required to demonstrate possession of unique knowledge agreed at, or items issued at, registration without disclosing anything that could be captured by an observer and replayed to falsify a transaction. Secure tokens (e.g. PKI certs), and one time passwords by phone or text message should be considered for authentication provision.	Services where the value is to the patient by having access to their records and empowering them to take better care of themselves and there is limited opportunity for fraud through the creation of false identities. For example, LTC portal or other Care Management related online service.
3	***Transactions in which substantial damage might arise from misappropriation of real-world identity*** ***Appropriate in circumstances where the service should be delivered to specific identified individuals and the risk of fraudulent use of the service is high.*** Provision of Level 3 personal registration services takes place largely outside the ICT. For example face-to-face registration and administrative verification.	Service authentication is required to collect strong evidence that the individual requesting the service is actually the person registered, and is present at the time of authentication. Tokens used in support of Level 3 authentication are typically smartcards, secure tokens, or mobile devices used in conjunction with a password/PIN.	Border controls and other physical access control. Financial benefit payments where the payments cannot be easily traced and recalled provide another example. Smartcard access to NHS systems and services. Services that attract a high level of personal accountability particularly where legal action may be taken against potential adversaries and evidence is needed that implicates the individuals concerned.

5. Identity Assurance Approaches – Key Steps

5.1. Conceptual components of identity assurance

In order to affect online access to services there are four end-user security components that are required for identity assurance:

- **Registration:** the act of establishing the identity of a subject as a condition for obtaining a credential that can be subsequently used to reaffirm an identity.
- **Authorisation:** the process by which a registered user's entitlement to access a particular service is confirmed and authorisation is then granted to access the service
- **Authentication:** [proving who you are] the process by which the electronic identity of a user is asserted to, and validated by, an information system on a specific occasion using a credential issued following a successful registration.
- **Privacy:** the requirement for the responsible handing of personal and/or commercially sensitive information by a service

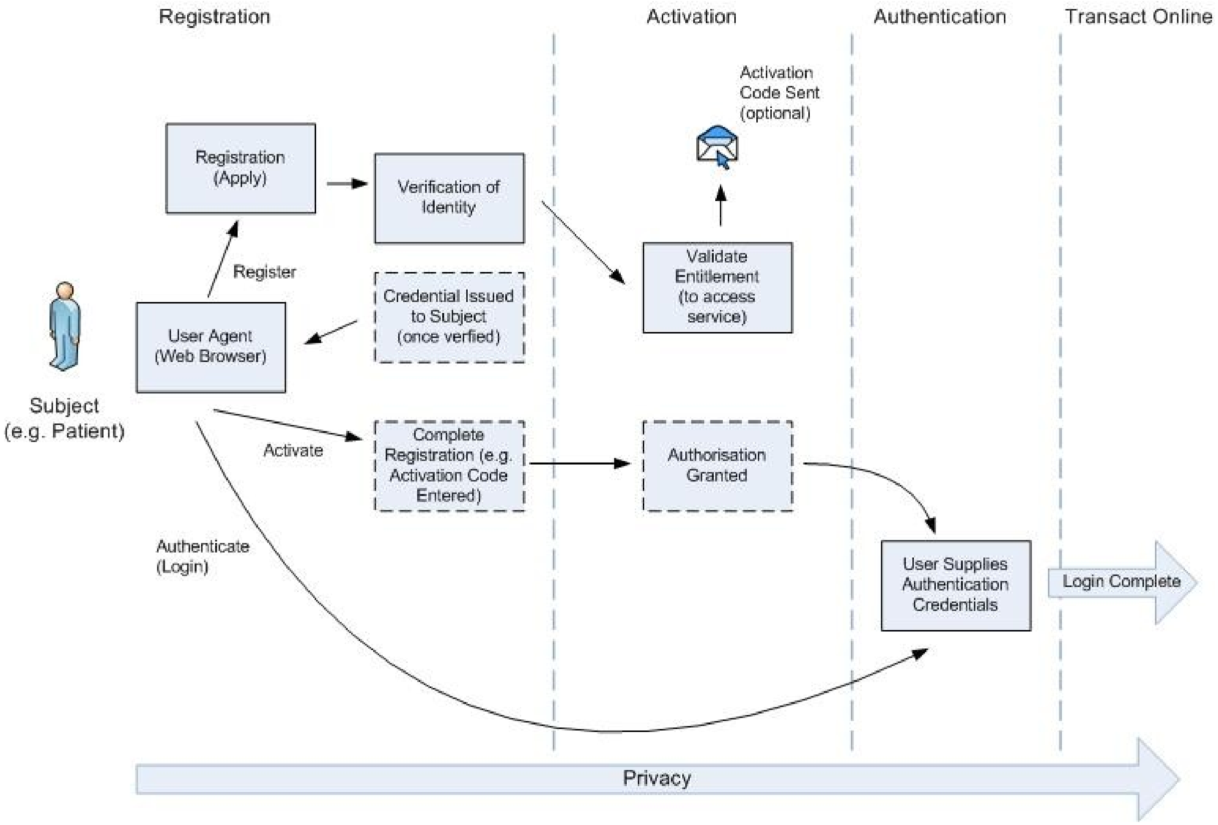


Fig. 5.1.1 – Key components in the identity assurance process

The guidance in this document focuses on the Registration and Authentication aspects of the Identity Assurance process. Authorisation varies depending on the Online Service being offered therefore only aspects that affect registration are covered in this document such as the issuing of activation codes. Privacy should be considered as much by the online service as the identity assurance provision therefore this is also omitted from this guidance.

5.1.1. Identity Assurance steps that should be considered

The key process steps in identity assurance are intended to cover a wide range of service requirements. In general, any service providing access to patient sensitive data (e.g. records) would require a more complete implementation of the steps described below.

Identity Assurance Process Element	**Service Providing Access to Patient Health Records or Patient Identifiable Data (Level 2/3)**	**Service including Personal Health Records[5] (Level 0/1)**
Registration	✓	✓
Verification of Identity	✓	
Validation of Entitlement	✓	
Activation (e.g. account activation)	✓	
Authentication	✓	✓
Privacy[6]	✓	✓

Fig 5.1.1.1 – Example of ID Assurance steps to be covered for patient facing services

5.1.2. Auditing and Protective Monitoring

Auditing and Protective Monitoring are requirements that are recommended for high assurance level scenarios (e.g. access to patient health records); however, auditing is recommended regardless of assurance level.

Identity Assurance Process Element	**Service Providing Access to Patient Health Records or Patient Identifiable Data (Level 2/3)**	**Service including Personal Health Records (Level 0/1)**
Auditing[7]	✓	✓
Protective Monitoring[8]	✓	Optional

Fig 5.1.2.1 – Auditing and protective monitoring

Other service specific precautions could be taken dependant on identified risk. For example, as part of protective monitoring usage patterns such as geo-location or moving from session to session rapidly may highlight an attempt to fraudulently access or subvert the service. Precautions for standard DoS attacks and other network-level attacks should always be applied.

[5] Personal Health Record: a health record held and maintained by the subject of care or a representative of the subject of care. This is not a centrally held NHS health record.

[6] Privacy requirements are dependant on the type of information gathered, stored or transacted.

[7] Auditing is recommended regardless of the assurance level required.

[8] Protective Monitoring is recommended where there is significant risk of fraudulent or inappropriate use or access to services.

5.2. Un-assured Website Accounts

This guidance focuses on online services i.e. 'websites' rather than identity assurance in general. There are a range of approaches taken to website user registration ranging from highly secure online banking accounts baked by processes such as Know Your Customer (as used by the UK banking system), to unverified website registrations which are often the large-scale everyday social media and email accounts that we all use such as Google, Facebook and MSN.

Where no verification of the registering user's identity is completed we have no assurance that that person is who they claim to be and should bear this in mind when considering user registration and authentication.

Many websites allow users to create an online account i.e. registering your name, an email address, maybe a few personal details with a website so that it can be personalised or retain information about the user over time.

This model works well but provides no proof that the person registering really is the person represented by the name they have provided. For example, anyone can create a Facebook account in the name of Adam Cooper however, are they all the same Adam Cooper or indeed the Adam Cooper who has a relationship with Dr Goode at the Wellbeing Clinic? We simply cannot know as no proof of identity was required to create the account.

Identity Assurance provides services with a level of assurance when transacting online which is based on the steps taken to prove identity during registration and the type of credentials used to authenticate (e.g. username and password is less secure than username, password and PIN).

The key difference therefore between Identity Assurance and unverified website accounts is that Identity Assurance allows the service to have a level of assurance that the person authenticated has proved their identity in a recognised and trusted way, whereas an un-assured website account is simply a self-asserted registration with a service and can be created in any name without check.

5.3. Proving Identity / Registration & Verification

Assuming that the service in question is to provide access to sensitive information or patient health records then we must consider the need to correctly identify the individual requesting access to that information. Standards such as eGIF provide guidance on this: *[to obtain] eGIF*[9] *level 2 registration, additional independent identity corroboration is required by using information considered private to the individual*.

Verification of identity can vary from asking the registrant to confirm something private which can be corroborated such as National Insurance Number or requiring the individual to present

[9] eGIF (e-Government Interoperability Framework) – http://interim.cabinetoffice.gov.uk/govtalk/schemasstandards/e-gif.aspx

ID documentation in a face-to-face registration. Banks often use this approach to increase their level of assurance by asking for recent transactions, overdraft limits, or types of account held as this is information that is private to the individual but also known to the organisation asking the question.

Note: It is recommended that local organisations undertake, document and refresh their information risk assessments regularly to ensure these remain accurate and continue to inform the security design and risk countermeasures for the assets concerned.

5.3.1. Verifying identity where a patient / clinician relationship does not exist

In order to ensure that the identity of a patient is verified to a high level of assurance it is necessary to corroborate registration data with multiple trusted data sources and taking steps to mitigate fraudulent activity. An example of how this could be achieved would be: matching demographic information to a centrally governed data source, cross-checking residency with a 3rd party data source, and the posting of an 'activation code' to the claimed residential address.

In order to reduce fraudulent registrations and to strengthen the verification process a strong address verification scheme should be considered for services providing access to sensitive information such as patient health records.

Verification that the person registering is resident at the given address ensures that:

- The claimed address is the same as that registered on a government dataset (e.g. PDS via a GP practice), matched against surname, DOB, postcode and gender;
- The claimed address is corroborated by a commercial identity verifier;
- The applicant physically resides at the claimed address through posting of registration activation codes to the claimed and validated address.

This approach provides:

- strong protection against fraudulent application from a physical address other than the current residence of the target applicant;
- protection against fraudulent application from non-family members resident at the same address. (Another resident would have to obtain private information regarding the targeted person, and intercept their mail.)

5.3.2. Verifying Identity where a patient / clinician relationship already exists

In a healthcare scenario there is often an existing relationship between patient and clinician(s) which can be used to reduce the overhead of proving identity. The Royal College of General Practitioners propose that *"The extent of identity checks can be supplemented by, or* *combined with, the healthcare organisation's existing knowledge and relationship with the patient."*

Where an existing patient/clinician relationship exists invitations may be sent directly to patients inviting them to complete a registration seeded from existing data sources negating the need for presentation of ID documents.

For example, the Choose and Book service allows a GP to register a patient to use the booking system during a consultation creating as part of that process an appointment letter containing a unique reference number for access to the online service.

- The GP registers the patient with the service and issues an appointment letter including a unique reference number and password
- Using the unique username and password credentials (alongside birth year) the patient is able to login to the Choose and Book Service online

This approach may be used by clinician's other than a GP where a genuine relationship exists between patient and clinician although it is most likely that a GP will be the primary point of access for most patients. The process employed to audit this method of registration should include strong checks that the clinician and patient have an existing professional relationship e.g. registered GP practice on PDS.

5.4. Mitigating the risks associated with registration

The potential risk of not verifying a patient's identity before granting access to sensitive information or records is dependent on the nature of each service but in general services that provide access to patient identifiable data or records should aim to mitigate the following risks:

- Fraudulent application
- Interception of Post or Email
- Collection of data from user workstations

5.4.1. Example Mitigations

A local assessment of risk should always be conducted regardless of the type of service being proposed. DHID currently recommends referencing the current e-GIF standards although other approaches such as RSDOPS may additionally be referenced if a cross-government approach is being taken.

The following are examples of the steps that could be taken to mitigate the risk of patient information being accessed inappropriately:

Risk	**Mitigations (Suggested)**
Fraudulent Application	• Registration information only posted to verified claimed address of applicant. • Claimed address verified by external address verification service. • Post redirections can be checked by external address verification service provider. (However need to consider impact on legitimate redirections). • Registration post does not externally identify the Service or that this is a registration document.
Interception of Post	• Information contained in Registration post is not sufficient by itself to enable registration. • Registration letter clearly states that it is insufficient by itself (to avoid negative press publicity). • Posted envelope does not identify that it has come from NHS or the Service (e.g. LTC Portal) and should not include any return to sender address.
Interception of Email	• When using email to amend account details such as password changes it is recommended that the user is also required to answer memorable questions to complete the account change. The memorable questions should be carefully considered and not the type that can be easily guessed in conjunction with online social networking sites.
Collection of data from user workstations	• Malware on the user's workstation could collect the data entered during the application and data presented to the user. During registration this information is insufficient to gain access to an account, since the activation code will be posted to the applicant's registered address however, all activation codes should be one-time codes to eliminate replay attacks.

5.5. Authentication Guidelines

The Authentication method used should reflect the 'value' of the information being protected and the level of assurance required by a service when identifying a person (or user).

The need for robust authentication methods has received recognition in the industry. An example of this is The Royal College of General Practitioners who note in their recent report[10] that:

> *It is recommended that two-factor authentication is used before enabling Record Access to provide an acceptable and stringent level of security that aligns with national standards. The two factors can be something known to the individual (PIN/password) and something they hold (card or token or mobile phone that generates random numbers). Shared secrets, using carefully pre-selected questions, can also be an acceptable method of authentication.*

Credentials and methods of authentication also differ greatly in their type and effectiveness and should be carefully considered when selecting products or mechanisms for 2-factor authentication. Additional guidance should be sought from a technical authority such as CfH Identity and Access Management if required.

Functionality of the service being protected should also be considered when selecting a method of authentication. Portals which provide access to a single patient record (i.e. the patient registered can see only their own records) pose a much lower risk than services that expose the records for multiple patients to clinicians.

The NHS HealthSpace portal which provides access to the Summary Care Record, currently requires users to login with a two-factor authentication comprising of username, password and random PIN number derived from a physical token (in this case a simple matrix card.) This is a common approach with secure online systems that are used daily, such as banks, requiring customers to use multiple factors, PINs, pass-codes and passwords to access sensitive information or to access transactional services.

Services which provide access to less sensitive information may simply adopt the username/password model or as is becoming more common simple authentication federation via large scale online services such as Google, Facebook, and Microsoft LiveID. The authentication used by these services is often only a single factor (e.g. password) but is improving, for example, with the introduction of Google 2-Step[11] verification which uses a mobile device or land-line to add an extra factor in the authentication process. It should be noted that many of these simple federation services do little to verify and prove identity therefore each should be considered only if they mitigate concerns raised by a risk assessment of the proposed patient portal.

[10] Enabling Patients to Access Electronic Health Records (Guidance for Health Professionals): Version 1.0 – September 2010 [Brian Fisher, Richard Fitton, Amir Hannan]

[11] Google 2-Step Setup – http://support.google.com/accounts/bin/static.py?hl=en&guide=1056283&page=guide.cs&answer=180744&rd=3

5.5.1. Protecting Authentication Credentials

Regardless of the number or type of credentials (factors) used to authenticate care should be taken to ensure that accounts are not compromised. In addition to infrastructure and application level security considerations the following suggested actions should be taken to reduce the risk of unauthorised access to patient data.

Both eGIF and RSDOPS part 2 include examples of credentials that may be used for each authentication level and how this may be provided online.

Risk	Mitigations (Suggested)
Brute Force Attack	• Minimum password strength criteria should be set for user passwords • In addition a separate one-time password mechanism is recommended for account changes and activation codes.
Authentication Credential Compromised	• The method of authentication should include measures to reduce the likelihood of malware or shoulder-surfing attack. • Authentication credentials should be one-way encrypted • All authentication must carried out over SSL protected channels
External Attacks	• Authentication screens should be subjected to penetration testing to establish that the screens and http exchanges cannot be effectively manipulated. • It is recommended that users should be informed of their last logon time when they authenticate. This will provide the potential for a user to detect unauthorised access, which may be due to their own lax protection of their authentication credentials. • Communications should inform users that they will never be legitimately asked for their authentication credentials. • To reduce the risk of eavesdropping all authentication data must be protected by encrypted SSL sessions.

6. Appendix A: Overview of proposed xGov Identity Assurance Approach

The Cabinet Office's IDA Programme is an Identity Assurance programme dedicated to the provision of a pan-government system for secure access to government services online, which:

- Provides citizens with a safe and secure means of registering their Identity for use with multiple digital services
- Provides government with a trusted means of authenticating these citizens when using a digital identity with a government service provider (e.g. an LTC Portal)
- Ensures that registration information (how the identity is proved) is neither duplicated or shared (with digital services)

In essence IdA provides the following mechanisms based on industry standards and proven protocols:

- Identity Registration – allowing citizens to register their identity for use when accessing government services online.
- Authentication – enabling citizens to securely authenticate their identity (i.e. log-in) in order to access a government service.
- Enrolment – a means of matching a citizen's 'Identity' to a government service provider's local records (e.g. matching to NHS number using the Personal Demographics Service – see Key Terminology below).

To achieve this, IdA will take advantage of existing identity providers (e.g. The Post Office) to manage registration & authentication, and proven technology standards to ensure security and level of assurance:

- ***The Citizen has choice*** – a range of identity providers will be available (such as The Post Office, PayPal and Experian) providing differing registration and authentication methods allowing the citizen to choose the most appropriate route.
- ***Identity information is not shared*** – registration details remain with the Identity Providers and are not shared with the government service providers. Government services merely know that the identity is asserted to be valid and at the correct level of security.
- ***Service Account Details are not shared*** – information recorded about an individual whilst transacting with a government service are held separately from identity information: in fact identity providers do not even know which service they are providing authentication for as part of a transaction.

6.1.1. Architecture Overview

The IDA programme utilises a Federated Identity approach separating Identity Providers (those who register and verify identities) from Service Providers (who consume assertions of identity from identity providers). This is a standard pattern commonly seen online with the proposed architecture built upon the proven SAML2 profiles and protocols. Major vendors already have products that support SAML2 identity federation and are currently engaging with the Cabinet Office to develop solutions.

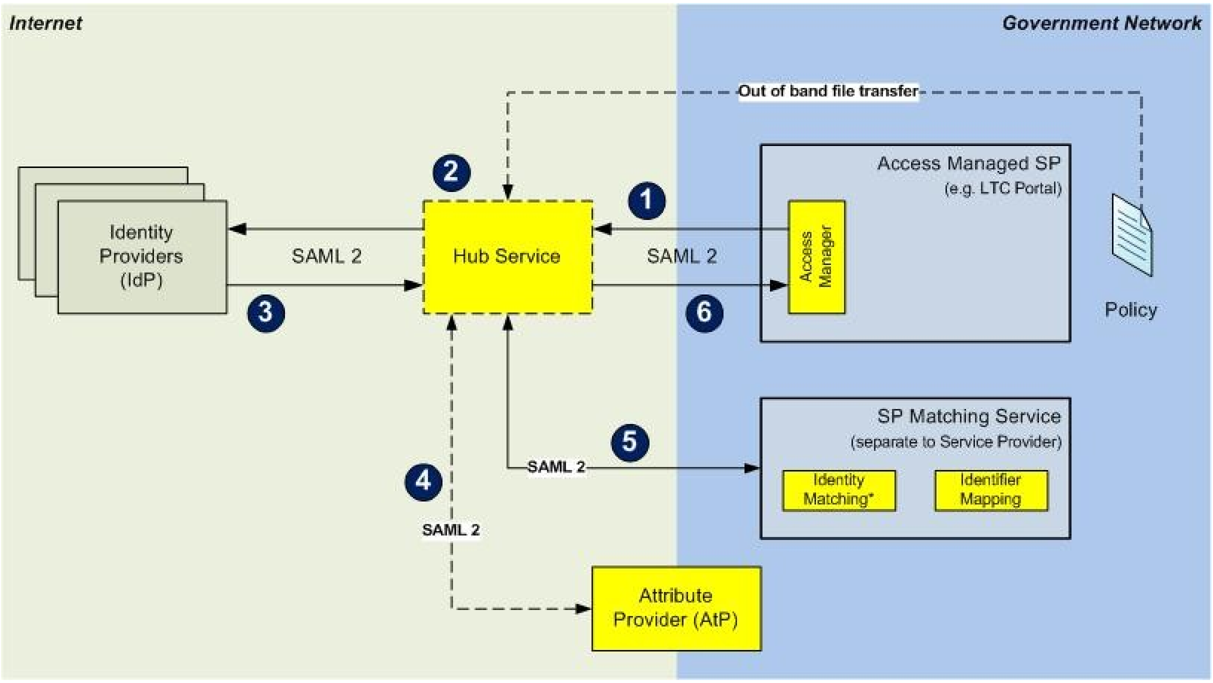


Fig. 6.1.1 – High level IDA architecture example

The following steps are taken to authenticate a person wishing to use a government service:

1. Authentication request is sent to Hub Service and user redirected to the Hub page
2. The user (e.g. a patient) selects an Identity Provider (IdP) from the Hub page and is redirected to the selected IdP
3. The user authenticates with the IdP and an assertion of identity sent to the Hub Service including a Matching Data Set (MDS) which will be used to match to a government data set (e.g. PDS)
4. The Hub Service (based on the Service Provider's Policy) requests additional attributes from government attribute providers attaching these to the full assertion of identity
5. The Service Provider Matching Service (SP-MS) receives the assertion of identity and the Matching Data Set which it uses to match to a local account (e.g. an LTC patient account)
6. The Hub removes the matching data set and asserts the completed authentication to the Service (e.g. an LTC portal).

6.2. Current Plan for Cross Government IDA Implementation

The IDA Programme has already delivered v1.0 of the technical design which has been used by DWP to implement a beta identity assurance solution and embark on the next phase of development for Universal Credits.

The Department of Health Informatics Directorate is working closely with the Cabinet Office Identity Assurance Team to ensure that the needs of patients and Health related settings are included in cross government thinking. We are playing a leading role in the technical architecture design process despite not being an early adopter of any subsequent Identity Assurance capability across HMG although we would expect to be a consumer of Identity Assurance services once they are widely available.

The Identity Assurance services defined by the IDA Programme will be available for use by other government service providers by mid-2013 although the strategic approach and technical design is already being adopted by some departments.

- DWP is intending to have a fully operational and tested implementation in place for Q1 2013 in time for the first public use of Universal Credits.
- HMRC is currently working towards convergence with the strategic architecture and is conducting a viability project for the first phase of work.
- In parallel, the Skills Funding Agency is developing a partially compliant solution which utilises the protocols and approach of the strategic solution without the Hub architecture (a single IDP is being used) which will be launched in 2012.
- DHID is currently playing a leading role in the technical design for IDA and would expect to utilise these cross government services as a national enabler for NHS IT projects in the future.

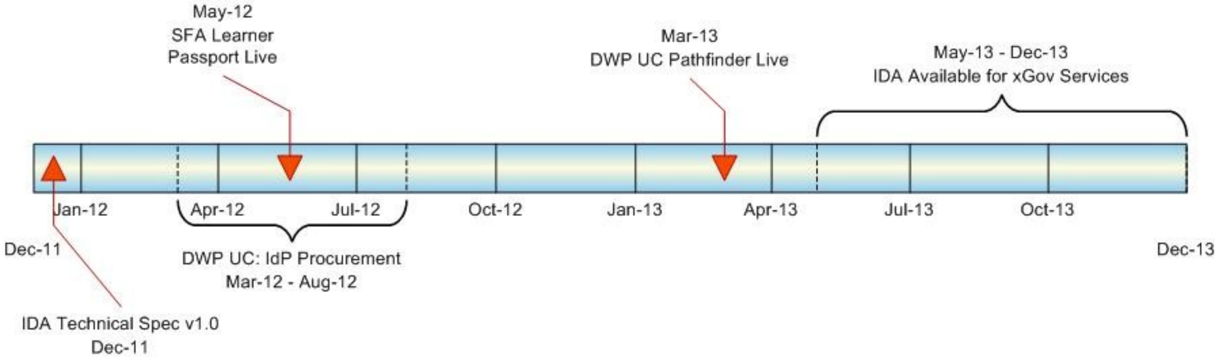


Fig. 6.2.1 – Timeline for IDA availability and associated programmes