SIGNING IN TO ONLINE SERVICES
The secure and easy way to access your public services online:

myaccount

Policy Privacy Impact Assessment Report

November 2014
Version 1.4
(Version Control at Annex B)
INTRODUCTION
This Privacy Impact Assessment (PIA) is being undertaken in response to development of policy for a national approach to secure and easy access to online services\(^1\). The policy will be implemented through the use of existing assets and processes of ‘myaccount’ (previously known as the Citizen Account).

This policy PIA used the ICO’s *Conducting Privacy Impact Assessments Code Of Practice*\(^2\) screening questions to help assess the areas the PIA should address. The answers are at Annex A. The main body of the report follows the format of the Code’s Privacy Impact Assessment template.

OVERVIEW
The need for a PIA
In line with good practice (promoted by the ICO and also by the Scottish Government’s *Identity Management and Privacy Principles*\(^3\)) this PIA is being undertaken as part of the development of policy regarding secure and easy access to on-line services.

Scope
This PIA relates only to the policy aspect of a national approach to verification and sign-in. There is a separate PIA\(^4\) covering an associated Information Assurance (IA) and Information Governance (IG) review that relates to the detailed operational arrangements that support this project’s policy aims. That more detailed document addresses the technical refresh of the technical platform on which myaccount runs, including details of Data flows.

To support delivery of the policy a need has been identified for secondary legislation to allow for a key reference number (the Unique Citizen Reference Number, or UCRN\(^5\)) to be used by public sector organisations not currently covered (‘prescribed’) under existing Regulations. A public consultation will be undertaken on the proposed amendments to The National Health Service Central Register (Scotland) Regulations 2006, which includes allowing organisations outwith local authorities and NHSScotland to be able to access the UCRN and use myaccount.

\(^1\) Scotland’s Digital Future - Delivery of Public Services
http://www.scotland.gov.uk/Publications/2012/09/6272

\(^2\) http://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment

\(^3\) Identity Management and Privacy Principles
http://scotland.gov.uk/Publications/2010/12/PrivacyPrinciples

\(^4\) www.improvementservice.org.uk/library/download-document/4076-myaccount-
privacy-impact-assessment-version-2/

\(^5\) The Unique Citizen Reference Number (UCRN) is used to ensure no duplicate records or accounts are created in your name. It is a 19-digit number that is generated using a special algorithm and is completely anonymous. The number is created by National Records of Scotland. If you were born in Scotland, your Birth Registration Number is used to generate your UCRN. If you were born elsewhere, a specially allocated number (in the same format) is used for your UCRN.
We will use responses to further assess any potential privacy impacts relating to the proposed expansion of the use of myaccount.

**WHAT THE POLICY AIMS TO ACHIEVE**

(a) To provide individuals, where the individual chooses to access services online, with the ability to have one username and password which supports secure and easy access to online public services provided by the Scottish public sector.

(b) To re-use and build upon existing assets to provide a national solution which can be used by all Scottish public sector bodies.

(c) To take into account a draft EU Regulation\(^6\) which aims to allow EU citizens the ability to transact online using mutually recognised verification and sign-in processes. The Scottish Government policy is to have a verification and sign-in facility that uses technical standards consistent with those that are likely to allow for interoperability within a federated model.

**Benefits to organisations and to individuals**

The secure and easy way to access your public services online

To meet growing demand from individuals and businesses, Scottish public sector organisations want to make services - information and transactions - available online. For example, for most people it is much easier if they can pay their Council Tax online or request a car parking permit without having to visit an office, a Pay Point or send a letter or cheque. When you undertake a transaction online you must be confident that your personal information is secure and that someone else cannot pretend to be you online.

This PIA is concerned with the incremental change from the existing use of the Citizen Account (CA) (now ‘myaccount’) and how myaccount will allow individuals to access public services easily and securely by creating their own myaccount through mygovscot (a Scottish public sector portal run by the Scottish Government). For more details on mygovscot\(^7\) please visit [www.mygovscot.org](http://www.mygovscot.org).

The Scottish Government has agreed this approach with the wider public sector (‘Service Providers’).

Individuals and organisations will also benefit from the way in which the limited sharing of the UCRN, undertaken following ‘privacy by design’ principles, can help a Service Provider more confidently know that the records it uses to service an individual’s needs relates to a specific individual. There is an associated messaging service which can help to keep core aspects of an individual’s records up-to-date.

---


\(^7\) [www.mygovscot.org](http://www.mygovscot.org) (available from 7 April 2014).
(using a consent model). For example, if an individual has consented, a change of address notification can be sent to service providers.

Having accurate and up-to-date records is part of an organisation’s obligations under the Data Protection Act (DPA). By adopting this national approach, which will be compliant with the proposed EU Regulation described above, providers will meet any obligations on them in that respect.

WHAT DOES ACHIEVING THIS MEAN?

What’s staying the same?
The policy is to use existing practices for a new on-line environment, therefore privacy elements are unchanged.

- A PIA was undertaken (2008) for the Citizen Account.

Choice
Our ‘Digital First’ policy is that people should choose to transact on-line because they find it easier to do so, i.e. a matter of choice. Individuals will thus choose to create a myaccount. If service providers find there is a demand for separate, service specific, sets of credentials (user name and password) then it will be open to them to offer this.

What will be different?
Wider use of myaccount

- The key change is the wider use of the myaccount for access to online services. Until April 2014 the main use of the Citizen Account has been to support issue of the National Entitlement Card which provides access to local government services and Concessionary Travel. We plan to make the myaccount available for access to all Scottish public sector services which require verification and authentication of identity.

Use of the UCRN – legislation changes needed

- The Unique Citizen Reference Number (UCRN) can be used by organisations ‘prescribed’ in the National Health Service Central Register (Scotland) Regulations 2006 (the “NHSCR Regulations”). The NHSCR Regulations

---

8 Data protection principles 
http://ico.org.uk/for_organisations/data_protection/the_guide/the_principles


10 Scotland’s Digital Future - Delivery of Public Services 
http://www.scotland.gov.uk/Publications/2012/09/6272

currently prescribe Councils and Health Boards. We will need secondary legislation to enable use by other parts of the public sector.

POLICY – AN INCREMENTAL CHANGE

Policy
The scope and depth of this PIA and compliance check is set in the context that:

- Operationally the key processes (i.e. data flow and the use of identifiers) remain the same (see ‘what’s staying the same’).
- The policy to have a national approach to secure and easy access to your public services online\(^\text{12}\) builds on a Modernising Government Fund (MGF) programme (Customer First) and its supporting technology (the Citizen Account).
- MGF stated (Oct 2004)\(^4\):
  - ‘…The focus will be on service delivery from single points of contact, providing access to secure electronic customer records (reducing the demand for customers to repeatedly provide the same information).’
  - ‘...deliver a secure framework for different parts of the public sector to share and exchange critical data…’
  - ‘We want to continue to develop online information and online, self-service transactions.’
- The process and system has been operational for several years. The Citizen Account underpins delivery of the National Entitlement Card (NEC) and is already being used for authentication of diabetes patients over the Internet and by the City of Edinburgh Council, since April 2014.

Step two: Describe the information flows

information flows
The policy for this national approach to secure and easy access to your public services online is that:

- myaccount only holds a thin mandatory set of personal information;
- There is a separation of myaccount data and transactional information (details of the activity being undertaken). Local Service Provider systems will be where the transaction records stay.
- The UCRN (the unique anonymous identifier for each myaccount) is

\(^{12}\) Scotland’s Digital Future - Delivery of Public Services
http://www.scotland.gov.uk/Publications/2012/09/6272
not used as a Persistent Identifier. The UCRN will only be used to match at a high level with a service provider’s records.

- The information architecture helps to protect an individual’s privacy: the UCRN at the centre (where there is no transactional information) in combination with no UCRNs within Service Provider systems (deeper than is needed to make a match).

- Messaging (updates in change of circumstances or key life events) must only happen in line with a “consent to share” data model.

These aspects of the policy and myaccount are consistent with the Scottish Government’s Identity Management and Privacy Principles.

The detailed information flows (and the use of identifiers to match records) that support a myaccount are described separately in the PIA\(^1\) of operational processes.

**Governance**

Governance for policy development and implementation is provided by the Digital Public Services Programme Board for National Level Actions. Oversight of operational delivery of myaccount is provided by the Improvement Service (IS) Board. Scottish Government is a member for the purposes of oversight of myaccount.

Governance at a more detailed operational level is supported by:

(a) NHS Central Register (NHSCR) Governance Board\(^1\), chaired by the Registrar General. This board oversees all work relating to the NHSCR.

(b) The National Services Scotland (NSS) Privacy Advisory Committee\(^2\) (PAC) is an advisory committee to the Board of NHS NSS and to the Registrar General. It is an independent committee which provides advice on requests for the release of patient identifiable information. In the coming months PAC will be subsumed into the new Public Benefits and Privacy Panel with a wider remit across the NHS in Scotland but its role advising the Registrar General will be carried on by the new panel.

(c) Regular operational meetings between the Improvement Service and NHSCR staff.

(d) The Information Assurance and Standards Management Forum (IASMF) which is an Improvement Service chaired board with membership from key delivery partners and Service Providers to consider Information Assurance and Information Governance matters. Its membership includes subject matter

---


experts. It promotes good practice and will interact directly with the NHSCR Governance Board and the wider Digital Public Services strategy governance groups\textsuperscript{16}.

(e) Daily operational governance is described in the Improvement Service PIA\textsuperscript{17}.

\textsuperscript{16} \url{www.scotland.gov.uk/Topics/Economy/digital/digitalservices/governance}
\textsuperscript{17} \url{www.improvementservice.org.uk/library/download-document/4076-myaccount-privacy-impact-assessment-version-2/}
Consultation - practical steps we have and will take to ensure that we identify and address privacy risks

Internal & external consultation

- *Scotland’s Digital Future - Delivery of Public Services*¹⁸ (the Digital Public Services strategy) was produced with cross-public sector input and was informed by consultation including that led by boards representing different parts of the public sector (e.g. local government). This is a high level strategy and does not specifically focus on privacy risks.

- Establishment of the short life Scottish Government chaired Identity Assurance and Authentication Working Group (IAAWG) which had membership from key sectors (including NHSScotland, Local Government, Scottish Enterprise and NRS) as well as internal Scottish Government representatives. This allowed for wider consultation with the public sector and included representatives with more specialised knowledge.

- The IAAWG considered privacy issues both from organisational and the customer’s perspective and ensured that the policy met these requirements. Members sought input from their sectors as appropriate.

- The IAAWG recognised that customers should have to opt in to use the myaccount and associated processes and at all times gave consideration around ensuring the policy includes: giving individuals choice; meets existing policies; (e.g. *Identity Management and Privacy Principles*¹⁹) and that data is handled appropriately.

- The IAAWG’s recommendations were considered by the wider Digital Public Services strategy governance groups²⁰.

- An explanation of the policy was set out on The Scottish Government Digital web pages and Blog²¹. This mechanism allows an opportunity for questions and comments.

- Next steps – public consultation on the proposed amendment to the National Health Service Central Register (Scotland) Regulations 2006 (Note there are a number of proposed amendments which do not relate to myaccount).

---

¹⁸ Scotland’s Digital Future - Delivery of Public Services

¹⁹ Identity Management and Privacy Principles
[http://scotland.gov.uk/Publications/2010/12/PrivacyPrinciples](http://scotland.gov.uk/Publications/2010/12/PrivacyPrinciples)


Step three: Identify the privacy and related risks

The following ten potential privacy risks have been taken from page 24 of the ICO’s *Conducting privacy impact assessments code of practice* as ones to be considered for this policy. Relevance and mitigating actions are set out below each risk.

**Risks to individuals**

1. Inadequate disclosure controls increase the likelihood of information being shared inappropriately.

   Policy set for the Improvement Service and its delivery partners (including Service Providers) is that controls must be in place. Sharing of personal information will only be undertaken with appropriate consent. The Scottish Government expects all parties to refer to the *Identity Management and Privacy Principles*.

2. The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people’s knowledge.

   The policy is specifically about secure and easy access to public services online and will not extend beyond that purpose.

3. New surveillance methods may be an unjustified intrusion on individuals’ privacy.

   Not applicable.

4. Measures taken against individuals as a result of collecting information about them might be seen as intrusive.

   The only information collected and held in a myaccount will be given by the individual for this purpose. The information does not include any information about service use.

5. The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.

   Sharing and merging: the only personal data shared is the narrow spine (described above). This requires consent.

   The UCRN is shared at a limited level. It allows service providers to check they are dealing with an exact individual, but the UCRN is not used as a Persistent identifier.

   The policy for this national approach to secure and easy access to your public

---

services online is that:

- myaccount only holds a thin mandatory set of personal information;
- There is a separation of myaccount data and transactional information (details of the activity being undertaken). Local Service Provider systems will be where the transaction records stay.
- The UCRN (the unique anonymous identifier for each myaccount) is not used as a Persistent Identifier. The UCRN will only be used to match at a high level with a service provider's records.
- The information architecture helps to protect an individual’s privacy: the UCRN at the centre (where there is no transactional information) in combination with no UCRNs within Service Provider systems (deeper than is needed to make a match).
- Messaging (updates in change of circumstances or key life events) must only happen in line with a "consent to share" data model.

These aspects of the policy and myaccount are consistent with the Scottish Government’s *Identity Management and Privacy Principles*.

6. Identifiers might be collected and linked which prevent people from using a service anonymously.

The policy seeks to provide access to online services. The solution will be used where there is a need for the service provider to know who the individual is. The policy does not allow anonymous use. However on-line access is optional and individuals can choose not to use it.

7. Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.

The policy seeks to provide individuals with a secure and easy way to access online services which require the service provider to know who the individual is. The individual will see what information is shared and if they do not wish to share the information then they can choose to interact with the service provider by an alternative means.

8. Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.

   (i) See 5 (above);
   (ii) Otherwise not applicable.

9. Information which is collected and stored unnecessarily, or is not properly
managed so that duplicate records are created, presents a greater security risk.

(i) Use of the UCRN avoids the creation of duplicate records.
(ii) The proper storage of information is part of the Improvement Service’s Information Assurance / Information Governance audit.

10. If a retention period is not established information might be used for longer than necessary.

Policy is that implementation and operation must comply with the Data Protection Act, which includes applying appropriate retention and disposal regimes.

---

Step four: Identify privacy solutions

Privacy Solutions

This policy PIA is concerned with setting a policy framework for secure and easy access to your public services online. It directs that its delivery is to be in a privacy-friendly manner. Its associated operational PIA is concerned with the operational processes to implement the policy and sets out privacy solutions.

---

Step five: Sign off and record the PIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

<table>
<thead>
<tr>
<th>Risk</th>
<th>Approved solution</th>
<th>Approved by</th>
</tr>
</thead>
<tbody>
<tr>
<td>That the policy does not direct privacy-friendly delivery.</td>
<td>As set out in this policy PIA – this is an incremental change to a system that was designed and has operated in a privacy-friendly manner.</td>
<td>Jane Morgan (SRO)</td>
</tr>
</tbody>
</table>

Step six: Integrate the PIA outcomes back into the project plan

Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?

<table>
<thead>
<tr>
<th>Action to be taken</th>
<th>Date for completion of actions</th>
<th>Responsibility for action</th>
</tr>
</thead>
<tbody>
<tr>
<td>The scope of this PIA is the policy framework. There are no specific resulting actions. The Scottish Government will use its membership of the boards (described above) to ensure that the policy is delivered to appropriate privacy standards. It has instructed the Improvement Service to undertake an operational PIA.</td>
<td>Ensured that the IS has undertaken a PIA on the operational design of the myaccount systems and processes. Ensure that the IS has undertaken (as part of its PIA) a DPA compliance check and IA / IG assessment. Published 30 April 2014(^\text{24}).</td>
<td>Jane Morgan (SRO)</td>
</tr>
</tbody>
</table>

Contact point for future privacy concerns in relation to the policy
dps@scotland.gsi.gov.uk

Linking the PIA to the data protection principles - compliance with the DPA or other relevant legislation, for example the Human Rights Act

Legal compliance was checked as part of developing this policy. The policy is compliant.

PRIVACY IMPACT ASSESSMENT SCREENING QUESTIONS

These questions are intended to help us decide whether a PIA was necessary. ICO suggests that answering ‘yes’ to any of these questions is an indication that a PIA would be a useful exercise.

**Will the project involve the collection of new information about individuals?**

Yes, it may – but only to increase the level of assurance of a myaccount if that is needed by a Service Provider.

The policy builds on the existing process (no further demographic information is asked for than has been the case operationally to date), but to enable people to increase the assurance level of their account they may be asked to set up secret questions and answers. Doing this will be a choice.

**Will the project compel individuals to provide information about themselves?**

No.

The policy is supporting access to online services. Online services are an option not a mandatory approach. Having a myaccount is a choice.

**Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?**

The nature of data held does not change but the system will deal with more individuals than at present – if individuals choose to access services online.

Data, as part of the verification and sign-in process, will be shared on a consent basis.

**Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?**

No.

The system which underpins myaccount is already operational and supports issue of the National Entitlement Card and is used for online authentication for the My Diabetes My Way programme.

There are very clear statements and principles around the setup and use of the account.

**Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.**
No.

Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?

No

The policy supports easier access to online public services by making it easier for individuals to ‘prove’ their identity once to the public sector, and then consume a number of services across the public sector domain without having to ‘reprove’ their identity. The myaccount service is concerned only with asserting identity – not with delivery of the actual services.

The policy supports the provision of secure and easy access to online public services; this is one a number of means to access public services.

Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.

No.

The policy is concerned with a verification and sign-in solution for the Scottish public sector. The principle underpinning the policy is that the minimum amount of information should be collected (no additional information beyond how the current system operates will be required).

Information separately collected by service providers as part of their online services (where verification and sign-in was facilitated as a result of the policy that this PIA is concerned with) is not part of this PIA.

Will the project require you to contact individuals in ways that they may find intrusive?

No.
## VERSION HISTORY

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 1.2</td>
<td>First Published Version (April 2014).</td>
</tr>
<tr>
<td>Version 1.3</td>
<td>Added link to the Improvement Service PIA (1 May 2014).</td>
</tr>
<tr>
<td>Version 1.4</td>
<td>Updated to reflect (i) Governance now in place; (ii) Public consultation on proposals to amend the National Health Service Central Register (Scotland) Regulations 2006 (November 2014).</td>
</tr>
</tbody>
</table>