Annex E: Consultation Questions

The consultation sets out a number of proposed amendments. Views are invited on the following:

1) Where data relating to a citizen is held it should be accurate.
Do you agree that the approach suggested at paragraphs 9-11 is an effective approach to achieving this?

Yes ☐ No ☒

If No, please describe the approach you feel should be taken.

We are concerned about these proposals because:

1. They would consolidate a national identity system for Scotland, with far reaching implications. The consultation in its present form does not provide a full picture of the implications of the proposals.

2. There are potential compliance problems with some of the proposals with UK data protection legislation and other information laws.

3. The proposed changes to the letter of the law would only affect a schedule of data flows and organisations, and not the main body of the legislation. But what is being proposed would require other modifications to the legislation to ensure it provides adequate governance and safeguards in its much expanded context.

4. The consultation response form asks a very narrow set of questions that do not allow for any fundamental questioning of the policy. Several of the specific data sharing arrangements contained in the proposals are not properly explained in the consultation documents, making it impossible to assess their implications. This is a very flawed consultation. Nevertheless, we have attempted to respond wherever possible in the structure of the questionary.

1. A national ID for Scotland?

The proposals centre on expanding both access to and the contents of the National Health Service Central Register (“the NHSCR”). The NHSCR holds the basic demographic details of everyone who is born, who has died or is (or has been) on the list of a General Medical Practitioner in Scotland. It is considered to be the most complete and authoritative record of individuals in Scotland. The register does not hold medical information, except for cancer patients and those who are part of specific research studies. The main official purpose of the NHSCR is to support the transfer of health records, but currently it is also used by local authorities as a population register.

In order to avoid duplication of records each individual in the NHSCR is
given a unique citizen reference number (UCRN). The Privacy Impact Assessment for the myaccount service linked in the consultation document claims that it is an opaque number that does not contain biographical references and is generated using a special algorithm by NRS. But according to other documents (http://www.gro-scotland.gov.uk/files1/stats/nhscr-rgb-4.pdf) it appears to be more or less the NHS number or birth registration number. This could make the privacy risks a lot higher. The consultation response should clarify what exactly the UCRN is, and how it is generated and maintained.

The stated aim of the proposed changes is to enable the approach to secure and easy access to online services (myaccount) to extend beyond services of Scottish local authorities and health boards to a wider range of public services.

The explanatory notes focus on the limited use of the UCRN and other data for matching identities at the front end authentication of individuals when they register for online services.

But the actual changes in the legislation would allow almost every single Scottish public body, including Glasgow Airport and the publicly-owned Caledonian Maritime Assets Ltd. - to check and correct any data they hold on citizens against the NHSCR.

Proposed para 9b in Schedule 2 would allow for widespread sharing of: “any other entry information which is equivalent to the information that has been provided by a body or person specified in Schedule 3 but does not match that information” with any “body or person specified in Schedule 3”.

The number is currently used by the NHS and local authorities, but the proposals would make the UCRN a key shared identifier used by up to 120 Scottish public bodies. This would consolidate the UCRN as a national identity number.

The Privacy Impact Assessment for the online registration system (http://www.scotland.gov.uk/Resource/0046/00465002.pdf) stresses that the UCRN is only used for temporary matching at the time of registration. But the consultation document reads as if it were persistent (e.g. “The attachment of the Unique Citizen Reference Number (UCRN) to a person’s data ensures that only a single record is held for each person. Where any information from the NHSCR is shared it ensures that there can be no mistake as to whom the information relates to”).

Even if the matching was temporary, all the secondary identifiers in each institution would be held together by the UCRN, and the organisations will also use the NHSCR to keep their records up to date. Therefore, even if the sharing of data was restricted to the moment of registration for online services, it would have much wider and long term effects in the administrative systems of participating organisations, paving the way for the creation of a national identity number.
The proposals do not include the creation of a national ID card, but the UCRN is already connected to the National Entitlement Card (NEC) (http://www.entitlementcard.org.uk/docs/TermsandConditions.pdf) through the Citizen Account Service. This provides Scottish councils with a facility to set up, verify and manage the electronic records of its citizens.

The consultation does not explain that the Citizen's Account national infrastructure database will contain an updated mirrored copy of part of the NHSRC (http://www.gro-scotland.gov.uk/files1/stats/nhscregb-4.pdf). Although the use of both the NEC and online services is voluntary, there is a detriment to those who don't use them. This is another step towards the creation of a national ID system.

In addition to the use of a single unique identifier across all government information systems, the proposals also centralise information about home addresses. The changes will allow for the sharing of address postcode and unique property reference number (http://www.aligned-assets.co.uk/addressbase/uprn.html)- UPRN, not to be confused with the UCRN - already held in the NHSCR with public bodies. The rationale is a vague expected improvement of service delivery. But combining the UPRN and UCRN allows the precise matching of people and places across Scotland. Attaching detailed address data to a unique identifier will increase the privacy risks compared to the latter on its own.

The case for widening access to NHSRC data should be a lot more robust, including estimates of benefits, safeguards against abuse and the details of the legal instruments that will ensure compliance with data protection legislation.

The consultation does not engage with these issues. It should be clearer about the implications of what is being proposed: a national ID system. The consultation documents structure the proposals around some expected benefits, but these do not seem to fully cover the effects of the actual changes in the law.

These proposals appear very similar to the proposals for a national ID system that the last Labour government tried to introduce at the UK level. These were rejected, but we are concerned that Scottish citizens will end up with such an ID system without any appropriate public debate.

In addition, official Scottish policy goes against such widespread data linking and requires strong safeguards against privacy abuse. In 2005 and again in 2014 the Scottish Government agreed to the “Identity Management and Privacy Principles” (http://www.gov.scot/Topics/Economy/digital/digitalservices/datamanagement/IdentityandPrivacy/IdentityManagementandPrivacyPrinciplesV2) which say:

*Public service organisations should not share personal information unless it
is necessary. If a public service organisation needs to link personal information from different systems and databases (internally or between organisations), it should avoid sharing persistent identifiers; other mechanisms, such as matching, should be considered. If a public service organisation believes that persistent identifiers should be shared, it must publicly explain why. …

The proposals in the consultation would go against this recommendation on the sharing of persistent identifiers, as a single persistent identifier, the UCRN, would be used across up to 100 Scottish authorities, backed up by use of the NHS Register to form a national identity database.

2. Data protection issues

The consultation paper states that "in each of the proposed amendments outlined above the minimum amount of data would be shared for the specific purposes outlined". In addition "where an organisation wishes to take advantage of this legislation it will also require to have in place data sharing agreements to ensure that appropriate processes are put in place and followed and that the data is used for the specific purpose identified".

But the purposes are not specified anywhere in the proposed legislative changes and these safeguards are not written into law as far as we can tell. The amended schedules do not mention online services or any other purpose restriction.

The paper appears to assume that appropriate safeguards will be out in place by every single organisation. But this appears to be wishful thinking.

In addition to the general issues above, we wish to present to the consultation process several specific data protection concerns raised by data protection expert Chris Pounder, who is also a member of our advisory council (http://amberhawk.typepad.com/amberhawk/2015/01/proposals-to-expand-central-nhs-register-creates-a-national-population-register-and-significant-data.html)

1 **Compliance with Article 8 of the Human Rights Act**: there is a need for the Registrar General to demonstrate that the compilation of a population register is “necessary” in terms of a pressing social need; this is needed to ensure the processing of personal data in the Register is lawful in terms of the First Principle and “necessary” in terms of a ground in Schedule 2 of the DPA.

2 **Consent**: the consultation mentions that some information held by local authorities are “added to the NHSCR when individuals consent”. The Data Protection Regulation is expected to state that public bodies can only process that personal data which is “necessary” for their functions. This means that consent cannot form a proper Schedule 2 basis for a public authority to share
personal data as it implies that such sharing is “not necessary” for their functions. That is another reason why the Article 8 position is important.

3 **Compulsion**: the consultation fails to specify how the NHSCR is to be populated to include the missing 70% of the population. One presumes it is through the use of powers in section 57 that require those who bodies that use the NHSCR to contribute to the NHSCR. On the other hand, it could be gradual accretion of entries over a number of years. Most data subjects have to use public services; they are therefore compelled to provide their details to a public body that might be compelled to pass them to the NHSCR.

4 **Cancer**: The consultation document does not identify that personal data in the NHSCR relating to “people who are registered as having had cancer” (see list of NHSCR items above) are Sensitive Personal Data; there is no discussion concerning processing/protection of such records.

5 **Retention of personal data**: if an individual moves to England one does not know whether his/her personal data will be retained on the Register. If someone moves home, is the previous Unique Property Reference Number or address retained? There is no mention of retention periods or what is retained.

6 **Data sharing**: the prospect of onward disclosure of personal data, by bodies that have access to the Register to those who do not have access to the Register, is not considered.

7 **Securing the register from misuse**: a centralised database will be a target for those who want to trace individuals in Scotland for whatever reason (e.g. some individuals might not want to be traced for legitimate security reasons) nor is there discussion about specialist circumstances (e.g. individuals who have undergone change gender might not want historic records kept). Identity theft is also an issue. Many of these security issues were explored during the UK ID Card debates in 2006.

8 **Audit trail**: No mention is made of what records are kept of access to the NHSCR and for how long. With the proposed UK National Identity Register of the Identity Card, it was this audit trail that created a record that linked to all the services an individual was using.

9 **Privacy Impact Assessment (PIA)**: The PIA linked to in the Consultation relates to “myaccount” and not the NHSCR. There is no PIA on the revised
NHSCR functionality described in the Consultation. As far as we can see the PIA on the current NHSCR has not been published (it should be according to the minutes of NHSCR Governance Board, meeting on 24 October 2013). The Minutes of 31 July 2012 states “KM raised concerns about whether some of the details in the Privacy Impact Assessment (PIA) were too confidential to be released”.

10 **General Identifier**: there are “General Identifier” powers in the Data Protection Act to define the lawful use of the Unique Citizen Reference Number (UCRN). There is no reference to the possible use of those provisions which would restrict use and provide further protections.

11 **UK Identity Assurance**: the proposed approach for delivery of electronic services differs from the approach of the Cabinet Office in London which requires no centralised identity database. The reason why the Registrar General’s needs a central register for identity assurance in Scotland but not in the UK therefore needs to be explained.

12 **Missing items**: the NHSCR is being linked with other personal data held by the Registrar General. For instance “over 81% of the Census records can be linked to an NHSCR record with reasonable confidence” (quote from “Linking the NHS Central Register Extract to the 2011 Census”; Paper 4 NHSCR GB (13) 04). Are links going to be developed to extend the NHSCR with data from other Registers? Are these personal data then going to be subject to sharing? These are unanswered questions.

13 **Transparency**: If trust of data subjects is lost, resistance to the proposals will increase and so will the risks to the NHSCR. Transparency is essential to keep data subjects on-side; any form of compulsion could kill the scheme. Transparency is served by dealing with the issues above.

3. Governance

The current regulatory framework under the Local Electoral Administration and Registration Services (Scotland) Act 2006 has put the NHSCR on statutory footing as a population register. But the proposed changes would change the nature of the register without any corresponding modifications to the wider governance and regulations about the data.

In addition the actual proposed changes to the letter of the law simply add some general data flows to a schedule without any strong constraints on purposes for which the data is to be used. The original act to be amended is potentially problematic, being too loosely drafted. Until now this appear not
to have caused practical problems. But given the huge expansion in the number and types of public bodies which will have access to the data it seems likely that problems will arise.

National Records of Scotland, as administrators of the NHSCR, on behalf of the NHS, will have a critical role as an identity provider. The situation in Scotland would be highly unusual in having a national archive and a health service being responsible for maintaining one of the most important databases on the government. In most countries this is the responsibility of the Interior ministry, which also tends to have responsibility for national security.

According to the consultation paper, the NHSCR holds address information for approximately 30% of the population. This data is added to the NHSCR when individuals consent to their local authority sharing this information with National Records of Scotland.

The consultation paper, in paras 9-11, focuses on the addition of address data by the NHS and the sharing of the UPRN and address postcode with local authorities and health boards. The stated objective for improving the quality of the data is to improve the quality of national statistics and research and service delivery.

As explained, NRS has access to postcode information provided by health boards (known as the CHI (Community Health Index) Postcode, but it is not currently permitted to hold this information in the NHSCR. The proposal is to integrate the CHI postcode into the NHSCR, presumably without consent as this has not been mentioned.

This is not objectionable in principle, but as we saw above the data could be shared more widely for a variety of different purposes with up to 120 public bodies in Schedule 3.

The amended schedules contain no restriction on sharing of UPRN or address postcodes. The reference database for UPRN is not exclusive to local authorities. Any organisation in Schedule 3, could buy the AddressBase database and use UPRN to check addresses in the NHSRC (http://www.aligned-assets.co.uk/addressbase/uprn.html).

The consultation should make clear that is is possible that all Scottish public bodies will have access to up to date detailed address data on any citizens they have on file.

Maintaining quality and accuracy of the information held on individuals is a principle of fair information processing, but at least as important is minimising access and sharing to what is necessary, and being transparent.

In relation to the stated aim to improve research and statistics, we would like to see more details on the processing of the data. At the UK level, the Office of National Statistics has strong safeguards against uses of data outside its
statistical remit, including for administrative purposes. The UK is also implementing a sophisticated system for the secure sharing of administrative data for research (http://www.esrc.ac.uk/collaboration/collaborative-research/adt/). The Scottish proposals seem very thin in comparison, which could increase the privacy risks.

The consultation documents focus on the use of data for online services through myaccount. But it is not clear why this particular approach has to be used for authentication. The British government, for instance, is creating a system based on identity assurance that does not rely on a single source of personal data (https://gds.blog.gov.uk/2014/01/23/what-is-identity-assurance/).

Authentication is not the same thing as identity. An authentication system can be created that doesn't automatically link to everything the government knows about a person.

2) We propose to extend the current ability to trace persons a) who go missing whilst in education and b) who should pay for treatment provided by the NHS. Do you agree with these proposal set out in paragraphs 12-13?

Yes ☐ No ☒

The consultation paper lumps together some disparate concepts in a very misleading manner. It conflates existing provisions for assisting in the search for missing persons by their family and friends, with proposals to assist public bodies tracing people missing from administrative systems. From a privacy and data protection perspective these are worlds apart, and the actual proposals involve expanding very different types of data sharing.

Solicitors and charities looking for missing people will be able to use address and postcodes to query the NHSRC, in addition to names as they do now. This does not appear to be problematic as long as there are enough practical safeguards.

According to the document, Scottish local authorities have legal responsibility for education and already use the NHSCR to track children missing from the education system. It is unclear in the paper whether they have a duty to account for every child or whether they chose to do so. The proposal would extend this data sharing to the UK Department for Education and local authorities in England and Wales.

Ensuring children receive an education is an important objective, but the proposals need more detail on the data sharing processes. It is unclear whether non-Scottish public bodies should be given access to such data on the basis of their legal obligations to ensure that all children are in education. In England and Wales it is the duty of the parents, not the State to ensure that children receive an education (http://www.legislation.gov.uk/ukpga/1996/56/contents). Local authorities have a statutory duty to make arrangements to enable them to establish the identities, so far
as it is possible to do so, of children in their area who are not receiving a suitable education. But this may not necessarily mean they have to track every child at all times. Children who are suitably home schooled would not fall under this category, for example. A database of all under-18s in England and Wales - called Contactpoint - was shut down in 2010 due to privacy concerns among other reasons.

The proposed legislative changes do not include any limitation to the tracking of children for a specific reason, and could potentially be used for many other purposes in the future.

In addition, we have received concerns from our members that these new provisions could be linked to the policy where every under-18 in Scotland will be assigned a “named person” who will have the power to “advise” and “inform” the child or handle matters about the child with the relevant authorities. The Regulations and LEARS Act already provide for access to children's data by all relevant parties and in our preliminary analysis it appears that the new proposals would not add any new data flows for named persons. But it would be very helpful if the response to the consultation clarified this point.

The proposal to share data with UK Visas and Immigration in order to trace people who receive treatment in the Scottish NHS without entitlement is not clear at all. It would appear that at present all "non-Scottish residents" must pay for their treatment, but the Scottish NHS has some arrangements to recover costs.

It is not clear whether this means recovering monies from the NHS of England and Wales. The paper states that if those people leave Scotland the Scottish NHS wants to be able to track them in order to bill them individually. But it is also unclear in the paper whether they mean people leaving both Scotland and the UK, or simply moving to England and Wales. It is also unclear whether British citizens would be treated differently from citizens of other countries.

While recovering unpaid hospital bills may seem reasonable at face value, it would be important to understand the full picture. This matching can only work if UK Visas also shares information back with the Scottish authorities, and the consultation should provide a lot more information on the mechanics and legality of this data flow.

3) In order to allow citizens to make use myaccount for a wider group of services (beyond health and local government), as set out in paragraphs 14-16, we propose to provide access to the bodies named in draft Schedule 3 (Annex B).

Are there any additional service providers who you feel should be included?

No. The number of public bodies included in the schedule is very broad and if anything already difficult to justify. For example, it is not clear at all why
organisations such as the Royal Botanic Garden require access to the data. The number and range of organisations that would be able to access the data is unacceptable.

Each single organisation requiring access to the NHSRC should make the case on its own merits, demonstrating the need and proportionality of the arrangement and how the data will be used in practice, including the protection and security measures the organisation will take.

4) Do you consider that the proposals set out in paragraph 18 are an effective method to identify Scottish Tax payers?
Yes ☐ No ☑

If No please describe the approach you feel should be taken.

The Scottish Rate of Income Tax (SRIT) will come into effect from April 2016 and HMRC will be responsible for identifying Scottish taxpayers and passing on the monies. The Scottish Government is seeking the ability to share NHSCR data – name, date of birth, postcode and gender – with HMRC to check that the individual resides in Scotland.

Collecting the right amount of taxes is a core function of government, and we would not want to see the public purse deprived of income. But data sharing for any purpose, however legitimate, must be both justified and fair. Unfortunately the consultation paper does not explain how the proposed process would work in any detail or the rationale for this particular arrangement. It simply says that there is currently no mechanism for identifying Scottish taxpayers, but not why other options are not preferred.

We have asked HMRC, who have explained that they are already able to identify Scottish taxpayers through their postcode. The NHSCR data will be used as part of a wider process to ensure the postcodes of Scottish taxpayers are up to date. HMRC will be communicating with affected individuals about this.

This process in itself is not very problematic, but it should be explained in more detail to ensure there are no creeping issues. For example, will HMRC be sending data back to Scotland to challenge discrepancies? Will the NHSCR incorporate HMRC data if the latter is more accurate?