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.

No

Accurate data about a citizen is known by the citizen.

Person centred approaches to individuals can create more trust, and be more effective.

In a recent speech Mr Swinney said " The Government believes in the privacy of its citizens, we will protect personal privacy, and I’m firmly committed to the fact that the internet is open and free and should remain as such."

Holyrood Magazine page 36 Issue 333 February 16th 2015

In October 2014 the Foreword of

Identity Management and Privacy Principles
Privacy and Public Confidence in Scottish Public Services

said –

To secure public support it is vital that we maintain and enhance Scotland’s reputation for the safe, secure and transparent use of data,......

This proposal to extend a unique persistent identifier called UCRN and the data attributes to hundreds of public bodies, and many potential thousands of medical researchers and many thousands of other organisations is not safe, does not have a PIA, poses an exponential increase in risk and potentially damages the personal privacy of all Scottish citizens.

As such, the content of the Consultation compromises "public confidence".

Sharing so much data via a Persistent UCRN means that people can trace who the individual is. MIT researchers report that just four fairly vague pieces of information — the dates and locations of four purchases — are enough to identify 90 percent of the people in a data set recording three months of credit-card transactions by 1.1 million users.

http://newsoffice.mit.edu/2015/identify-from-credit-card-metadata-0129

Anonymised Data is not anonymous - The examples above (along with others) show that analytic techniques can be used to identify individuals from many anonymised datasets. Along with other organisations, government cannot assume that anonymisation is sufficient protection for personal data.
Article 8 of ECHR also in the Case of I v Finland - The ECHR found that if personal data is
not secured adequately, and the State does not take positive steps to do so (and not
just legislation but technical and procedural steps as well), then the state is in breach of
Article 8.

It is a very risky database when all Scottish citizen's UCRNs can be used to link activities,
track people and potentially use personal data for companies or other interests. These
things are already happening and the results are of concern.

There should be a much wider public, open and transparent debate in Holyrood and
Westminster about the privacy and security of Scottish, UK and EU citizens, their personal
privacy and the other potentially dangerous impacts of this proposal and Consultation.

In the Identity Management and Privacy Principles, Para 2.1 states
d) personal data is only retained as long as is necessary (9) and subsequently destroyed in
a secure manner.

However, the Consultation proposes to keep personal data, and to link it to the UCRN and
other databases for a person's whole life. This is the opposite of the The Scottish
Government Principles.

By creating a Persistent Identifier i.e. the UCRN and tracking its use across all
Organisations in Scotland, the State is building a National Identity database, in which the
data, metadata and linking of transactions will enable the identification, linkage,
aggregation and tracking of all citizens.

It is possibly in contravention of EU and UK laws regarding privacy, and there is no explicit
consent sought from Scottish or other citizens to have their personal privacy compromised
by a large Scottish National UCRN Identity Database.

This Consultation should be brought before Parliament for a proper, fair and transparent
debate. It should also be accompanied by a Privacy Impact Assessment.

It also has an impact on all Scottish citizens as UK citizens, as our privacy in the UK is at
risk by the actions of a Scottish Government. This is a sort of " East Lothian Question " as
the Scottish Parliament is influencing the rest of UK and EU, rest of World visitors when it
attaches a UCRN and tracks them.

It affects all citizens in Scotland, and for visitors from elsewhere in the UK and EU and
therefore has far-reaching, significant legal implications for tourists, visitors, citizens, health
patients and young people as there is no clear guidance on age.

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 x □

If No please explain why not?
The treatment proposed is potentially inefficient and not in accordance with practice elsewhere in
EU and beyond.
As a country, Scotland should set an example and collaborate with learning from others e.g. Canada and Scandinavia to respect the personal privacy of the citizen. Scotland should have Personal Privacy Principles that prevent the personal information of its citizens being taken away and used without their consent.

Unfair Government policies have in the past set taxes, which have subsequently been written off and they can also set policies which can damage and harm the personal privacy of Scottish citizens where not enough debate and scrutiny takes place. There should be a much wider debate.

The changes would undermine the public’s trust in the NHS, by using it as a vehicle to deliver these proposals.

There are other ways to ensure that citizens in Education and Health offer sufficient information and evidence for Government to work. They do not have to involve these proposals.

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?

15: The myaccount operator (the Improvement Service) must be able to verify an individual’s identity before issuing credentials (a username and password) which allow an individual to be authenticated when they make use of online services. Basic personal data are provided by the individual when they register for a myaccount and verified against the NISCR, at which point the Unique Citizen Reference Number (UCRN) is attached to that personal data. This avoids the creation of duplicate myaccounts. Individuals can see the data held in their myaccount. Where an individual is authenticated by using their credentials, myaccount confirms identity to the service provider by giving the service provider the UCRN, or sufficient information to allow the service provider to know the individual is the person in their own records. This approach is set out in more detail in[15].

This Section does not state all the options available, or give the reader or Parliament enough evidence or options to make these statements. If there is a Privacy Impact Assessment, then citizens and the Parliament can consider the options in an open manner. The UCRN prevents the individual having personal privacy.

It would be better for citizens if the Improvement Service offers verified attributes to Scottish citizens in a way that is “privacy by design”, and citizens control their personal data. This would involve co design, collaboration and working with citizens in a democratic, collaborative way to find results and outcomes.

The suggested approach is the wrong way round. It does not ensure privacy or personal privacy as Mr Swinney says in Holyrood Magazine that he wants for the citizens of Scotland.

A UCRN is a Persistent Identitifier, and the Scottish Government Privacy and Identity Principles in 2010 rejected Persistent Identifiers as being too dangerous and creating risks to citizens.

By attaching and promulgating the UCRN across Scotland and the rest of the world, Scotland creates a giant honey pot of personal data for criminals and potentially dangerous exploitation by people who wish to compromise privacy and break cyber security.

By spreading the UCRN across 1000s of Organisations, places and Researchers etc. in Schedules 2
and 3, the State is proposing to give the personal data away, and then there is a risk that private companies that already serve the NHS, and other State entities will be able to access this data when one of the State entities or employees might in the future seek to sell, leak or lose personal data by accident. The press in the UK has also recently purchased such data from public sector employees and other sources.

In November 2013, Scottish health services data appeared in a USA software company 

MedRed, a Washington, D.C.-based healthcare software company, and BT, a UK-based telecommunications company, launched the health cloud Tuesday with the blessing of the federal government. The White House Office of Science and Technology invited MedRed and BT to present the MedRed BT Health Cloud (MBHC) at a big-data event Tuesday in Washington, D.C., in a move signifying the federal government's recognition of the importance of open data in healthcare.

The MBHC data was taken from the UK through the UK National Healthcare Service, as well as Wales and some of Scotland.

In Schedule 2 and Schedule 3, the only safe and secure and trusted legal entity to pass the personal data to, is the person himself or herself.

Then the person knows their own data is safe. The individual has personal control over personal data.

There are no other service providers who should be included, unless the individual gives their explicit consent. Otherwise the Scottish State risks losing all trust in its services, and its employees can sell, view or release personal data to anyone else by linking the UCRN.

This is what sometimes happens in hospitals, and is happening with journalists and the Scottish citizen does not wish to have a persistent, unique identifier track them for their lives.

People sometimes avoid public services because of stigma; people also can avoid using public services because of the fear of being identified and details being passed to other agencies. People avoided paying the poll tax because of fear, and many citizens “disappeared” from public records.

Holyrood Magazine Issue 333 February 2015 pp 36 -

Mr Swinney is quoted as saying "The government believes in the privacy of its citizens, we will protect personal privacy, and I’m firmly committed to the fact that the internet is open and free and should remain as such......”.

This Consultation directly contravenes his statement as it makes Scottish citizens’ lives completely non-private, as their data is exposed to 100’s of Organisations and is proposed to be shared with 1000’s and 1000’s of other people and Organisations.

The risks of data sharing and data loss have also been seen recently in the public domain with Police
Scotland and "stop and search". In this they claim to have lost 20,000 records of their "stop and search" activities of children and it is not sure how many others in Scotland.

Linking all these "stop and search" records to a UCRN would mean that a child was labelled for life, with a UCRN persistent identifier marking them as "stopped and searched". In such a way, no one would be safe from having their criminal record released or identified. It could compromise the policy of restorative justice, and forgiveness and compassion of the Scottish Parliament.

This risks contravening EU Law as Google has been asked by the Courts to allow people "the right to be forgotten".

Tagging people with their UCRN is therefore likely neither to be in compliance with Identity Management and Privacy Principles or UK or EU Law.

This centralisation using the UCRN, and significant increase in risk taking by sharing people's personal information is then at risk of criminal or other forms of extortion, compromises and increases risks because of a Scottish National Identity Database. The fact that it links persistent identifier UCRN data so that people can be tracked without knowing, and the risk then that further commercial interests can profit from personal private data sales from Scotland to elsewhere.

Scottish NHS data has already surfaced in USA and the Middle East through middle-companies and this Consultation will increase the risk to citizens of Scotland that their personal, private data is moved without their knowledge. Here is an article about Scottish NHS data making its way to the USA, and it is not known what data attributes may have been passed across from e.g.

- CHI number
- Diabetes record
- Cancer information
- Gender
- Date of Birth
- Address
- Name
- UCRN

All of this personal and sensitive information may be contained in the American and Middle East health research company’s records and data systems now.

It is unclear whether citizens in Scotland were asked to give permission. Once the data has gone, then it is certainly not easy to know where it will go afterwards.

But it would be much fairer to the people of Scotland, anc to the Parliament in Holyrood if people could be able to understand how NHS Scotland data is being sold or moved to other countries e.g. USA. The Consultation proposes that eventually all 5 million Scottish citizens’ UCRN details and potentially other personal private data being sent down the same channels to another jurisdiction, and thereafter on to crime and other entities that citizens in Scotland would not know about.

The MIHIC data was taken from the UK through the UK National Healthcare Service, as well as Wales and some of Scotland.

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. This will ensure that we continue to protect and control the use of the information within the NHSCR. Sharing of information from the NHSCR will continue to be at the discretion of the Registrar General.

This paragraph and Section is not complete as it does not state all the facts, nor does it state the consequences of a persistent identifier such as the UCRN being used across someone's whole life to track them and prevent their right to a private life. There must be a Privacy Impact Assessment.

Again the Identity Management and Privacy Principles state the following and are written in the updated Version 2 of October 2014. These Principles take a more person centric approach to individuals in Scotland and their personal data, and suggest that individuals can hold a Personal Data Store for reasons of Identity Assurance and other transactions.

The Principles also restrict data linkage, sharing and the dangers of exploitations by sharing with commercial companies e.g. medical and other agents who may mis-use personal data shared with them without consent by Governments —


Storing identifying information

4.5 Public service organisations must consider whether identifying information needs to be stored in a database at all. In some cases, it might be preferable for people to hold and manage their own identifying information which can be accessed by the public service organisation when it is needed.

Linking information between systems

4.6 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.

If minimum data is the UCRN, and it is a unique, persistent identifier, then people will quickly be able to identify who people are. It is not necessary to share the UCRN, and indeed it may be detrimental to an individual’s interests to do so.

As such, the Consultation contravenes the Scottish Government’s Identity Management and Privacy Principles.

Data Linkage 5.5

Procedures to link data should involve the separation of identifiers (e.g. name, or unique reference number) from the rest of the data, and consideration should be given to separating the indexing, linking and analysis functions and personnel. The linkage method used should be that which requires the minimum necessary identifiable data.

The default position should be that data users have access only to data from which names and direct identifiers have been removed, and data users should be subject to an obligation not to attempt to re-identify individual data subjects. Any request for researchers to have access to data containing identifiers should be fully justified and risk assessed. No attempt should be made to re-identify individual data subjects and doing so without the authority of the data controller would be in breach of the Data Protection Act.
As the Individual Citizen is the legal Data Controller of their UCRN, then the last sentence makes the proposals in the NHS CR Consultation potentially in breach of the DPA, as the proposals do not ask the Individual Citizen for authority or explicit consent as worded in the Consultation.

European law based on s8 ECHR right to privacy, clarified in the v Finland case

The applicant "I", now 48 years old, stated that her private medical records were accessed by the other people, who did not need to and as a result of which she possibly lost her job as a nurse.

The access, which occurred around 1992 was not recorded, as there was no records to record access to medical records in Finland in the early 1990s.

The ECHR decided that as the hospital was controlled by the State (Finland), the Finnish government was therefore responsible for the actions at the hospital and access to the medical records.

A key finding of the case was that the court stated that personal information relating to a patient undoubtedly belongs to his or her private life. Therefore Article 8, freedom to a private life, is applicable in this case. Based on this the European Court of Human Rights found that a person’s right to respect for their private life (under the ECHR,) may be breached where the State fails to take appropriate steps to secure data, so that it cannot be accessed improperly.

Article 8 not only means that the government must not interfere unduly into a person’s private life, but the government must also undertake positive actions to prevent such interference, e.g to produce or enforce systems and protocols to protect data.

This case is particularly interesting as there no statement that there was deliberate and unauthorized access of data, only that there was failure to secure the data appropriately. i.e a breach of Finland’s positive obligations under Article 8 of the Human Rights Act

**Summary:** The ECHR found that if personal data is not secured adequately, and the State does not take positive steps to do so (and not just legislation but technical and procedural steps as well), then the state is in breach of Article 8.

The Scottish Citizen is the only legal entity able, empowered and likely to determine whether their personal data is shared, not an organisation on a list of 1,000 of names that exposes huge risks to personal privacy. Schedules 2 and 3 threaten the personal privacy of all Scottish citizens, as they will be tagged with a Peristent Identifier and this will be passed between Government Organisations, and passed outside to others and be exploited.

This will damage trust in the Scottish Government.
Only the citizen should have personal control over their personal data, and they can then have control and choice to share their personal data.

What is an “appropriate process“? This requires much more definition and currently renders this paragraph incapable of being judged. There is not enough detail for this to be understood, as the scope is not clear and there is no assessment of the impact on personal privacy.

The Registrar General in Scotland should empower and assist Scottish Citizens by passing back to them their personal data e.g. birth certificates; marriage certificates; death certificates. Then the citizen can exercise personal control over personal data, hold the data in their own, secure place and the citizen can decide how, what and with whom to share. This is a fairer “social contract“, and will improve public services as it is built on trust.

This is what Mr Swinney said in his Speech and quote to Holyrood Magazine –

“We will protect personal privacy.....“

This Consultation endangers personal privacy. There should be much more open, transparent dialogue and discussion in Holyrood and Westminster to prevent this Scottish National Identity Database being created.

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

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

It is therefore proposed that NHS should have the ability to provide certain information - name, date of birth, postcode and gender - from the NHSCR to HMRC for the purpose of identifying that the individual resides within Scotland. Making use of the NHSCR for this purpose would mean there is no need to establish a separate register for the purpose of identifying Scottish tax payers.

Previously there has been no need to identify Scottish tax payers separately to UK tax payers, so there is currently no mechanism in place to do so. NHS is the most accurate register of individuals in Scotland. It is therefore proposed that NHS should have the ability to provide certain information - name, date of birth, postcode and gender - from the NHSCR to HMRC for the purpose of identifying that the individual resides within Scotland. Making use of the NHSCR for this purpose would mean there is no need to establish a separate register for the purpose of identifying Scottish tax payers. This data will be shared with HMRC solely for the purpose of identifying Scottish tax payers and a data sharing agreement will be drawn up to this effect.

It is highly unusual for a Health system in one country to be used for taxation purposes in another. This may contravene EU Law and an individual’s right to privacy. It places GPs in a difficult position as tax collectors, and without explicit consent the GPs may be breaking the DPA.

A Health system home address is often 3 – 12 months out of date, and it is often incomplete. To avoid tax in Scotland, there is a risk that people will choose to avoid going to the doctor, or give the wrong address in order to receive healthcare and avoid taxes. This is what happened with the Poll Tax – people disappeared to avoid it.

It is much more trusting of people to ask individuals to volunteer their personal information. If the matter is explained, then people can choose to give their consent.

As the Health system in Scotland currently only has 30% of the people and their details in it, then if GPs are to be used as agents of HMRC, there is a high risk that a number of Scottish people will avoid tax by not going to the Doctor.

GPs will have to be paid to become tax collectors, and trust in the medical profession will decline.
GPs are not trained to be home address tax inspectors, or to check on citizens for the Scottish Revenue Authorities and this will potentially be very harmful to the reputation of public services and break trust for a Scottish Government who “....will protect personal privacy....” according to Mr Swinney.

Rich people who should pay tax will find ways to avoid tax, and can use a private doctor, or cross the border if they have two homes. Then they will not have to register in Scotland, and Scotland’s Health System will become compromised as an agent of the UK tax collection regime.

It is difficult to envisage if these Scottish Laws for some people who may elect to be UK taxpayers, or who may only spend a day or a week in Scotland when they are ill, would be acceptable to the Westminster Parliament.

The Holyrood Parliament cannot presumably legislate for UK citizens in matters where it has no jurisdiction.

The proposals are therefore potentially “ ultra vires “ as they are not able to be considered by Holyrood.

The proposals are also potentially unworkable for the reasons given. Taxes are collected through PAYE and HMRC, ICAS, ACCA, CIPFA and ICAEW should be consulted, as should the GP community in Scotland.

This is a sort of “ East Lothian Question “ as the Holyrood Parliament is initiating Consultation that could be seen as attempting to take powers and bring influence over UK Tax legislation. The consequences will be multiple, and include that fact that the UK has a Scottish National Identity Database introduced in one of the four nations, and which the UK has maybe not envisaged for HMRC or any other purposes.

Visitors to Scotland will find themselves with a UCRN reference that may stay with them as a Persistent Identifier for their whole life, and for which they have not given consent.

It will be a risk for public services in Scotland as people may be advised that in order to protect themselves –

“ No Doctor, No Tax “ or “ No Doctor, No UCRN “ or “ No UCRN, No Doctor “

Health inequalities will possibly increase, as people will avoid the GP to avoid the UCRN and this will be unhelpful for citizens and politicians who will then have to find more budget for people who may have a worse health outcome or crisis instead of seeing a Doctor.

For these reasons, the Scottish Government should halt these proposals, and instead move to recognise these changes and context for what they are: a significant development in our Scottish citizens’ relationships with public sector organisations, requiring a full debate in Parliament, with the chance for both MSPs and the public to have a dialogue, and to scrutinise and change them.

Then there can be an opportunity for person centred public services to be included in the dialogue, and alternatives put in place to build a more collaborative way to maintain personal privacy in Scotland for Scottish citizens, and to co design and create a Scottish trust framework where individuals and organisations are able to work together to deliver services we want.