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.

   Comments * SEE SEPARATE 'COMMENTS' DOCUMENT

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 ☑

   If No please explain why not?

   Comments AS ABOVE *

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?

   Comments NO - AND AS ABOVE *

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.

   Comments AS ABOVE *
Consultation on proposed amendments to the National Health Service Central Register (Scotland) Regulations 2006

Comments - Dr John Welford

It should be said at the outset that the progress of this NHSCR scheme during the past decade seems to have been carried out in a remarkably secretive manner and without full and proper parliamentary scrutiny. How can it be that the people of Scotland and indeed their Scottish Parliament representatives should have remained so completely in the dark about these important developments and never invited to examine, comment on and approve the Scottish Government’s overall plans. This hardly provides an encouraging picture of the state of Scottish democratic accountability.

Furthermore, unhappily this consultation seems designed to continue in a significantly non-transparent mode. It’s obviously fine for four specific ‘closed’ questions to be asked of any proposal. But it’s surely absolutely essential that in addition there should be a fifth, completely ‘open’ question, such as: “Do you have any further comments to make”? But perhaps more pointedly in order to solicit valuable feedback the additional fifth question could have been: “What do you think of this overall scheme, and can you see any significant problems with it?”

The absence of such an ‘open’ question could be down to poor consultation form design. But obviously, more worryingly, it could indicate that there has been an inflexibility of thinking behind the NHSCR scheme. In other words, minds may have already been made up about the overall scheme a significant time ago, and so there is little interest in what people’s views about it may now be. Also perhaps there is a fear of subjecting ‘the big picture’ to close scrutiny, because it might just highlight embarrassing weaknesses in what has been implemented thus far and what is proposed for the future. If there are such design weaknesses, they clearly need to be highlighted and dealt with - and as promptly as possible.

The harsh reality, of course, is that large, costly government IT projects, as this one most surely be regarded, only too frequently have to be cancelled, from a mixture of faulty systems design thinking, unanticipated problems, over-complexity, delay and massive overspend. It is therefore essential that maximum transparency and maximum scrutiny by as many well informed people as possible should be exercised, so that the policy finally agreed is the best one available and that the systems design will be robust.

Conclusion The apparent burying of heads in the sand regarding the overall design of the NHSCR scheme and the conduct of the consultation is extremely worrying and can only bode badly for the ultimate success of this project. Especially when the Scottish Parliament and Scottish citizens themselves have been kept largely in the dark for more than ten years about what is going on and where this project is ultimately heading.

1. Terminology

There appears to be a serious problem with the terminology surrounding both this scheme and the consultation, which does not facilitate clear thinking and transparency.
My reason for using the term 'NHSCR scheme', is because the scheme overall has manifestly little to do with the NHS. As will be seen in the two systems diagrams from the Improvement Service in March 2008, the NHSCR (as then thought of) was already being seen as a peripheral database, with the 'National Citizen Account' database (as it was then referred to) seen to be at the very hub of the network, essentially acting as a National Identity Register. See Appendix and: http://www.jwelford.demon.co.uk/snek/JimKinneydiagrams.pdf

So why continue to risk confusion with the notion that the National Health Service Central Register should still be seen as an NHS Register? This register, administered by National Registers of Scotland, "is considered to be the most complete and authoritative record of individuals in Scotland" (p. 5, para. 6). The normally accepted name for such an all-encompassing national register is, of course, a National Identity Register (NIR), and so it is puzzling why this much more transparent name is being avoided, serving only to confuse. In what follows, I shall therefore seek to use the term 'NHSCR NIR', rather than just 'NHSCR', in order to more accurately describe the true status of this central register within the overall system.

There has also been a similar confusion regarding the smart ID card first introduced to pensioners and the disabled in 2006. This was initially introduced quite simply as 'the free national bus pass', and continues to be known as such by the vast majority of card holders. Unfortunately, there is still nothing on the card to indicate what it actually is, but the term National Entitlement Card has been in the small print ever since 2006.

The term 'National Entitlement Card' (NEC), was, of course, Labour Home Secretary David Blunkett's preferred name for the UK ID card, and so there is little doubt that the Scottish version introduced by Labour in Holyrood at about the same time was also itself a prototype ID card (although without the fingerprint and iris-scan biometrics proposed for the UK ID card). The card's key properties of having a unique national number (the UCRN - Unique Citizen Reference Number), being linked to an NIR and being multi-function would appear to confirm that this is indeed the case. However, the Scottish Government's reluctance to use the correct term is hardly surprising, given how much ID cards are disliked by the general population. Incidentally, the fact that Scotland's NEC card is voluntary and does not have to be carried in any way absolves it from being an ID card. For the UK ID card, when introduced, shared precisely the same two properties.


This document is referred to as follows in the present proposals (para 7, p 5): "Use of the UCRN [Unique Citizen Reference Number] is in line with the Scottish Government Identity Management and Privacy Principles document." However, no explanation or justification for this statement is provided.

2.1 Persistent Identifiers

What the 'Principles' document does say (para 4.6, p 9) is: "[Public service organisations] should avoid sharing persistent identifiers; other mechanisms, such as matching, should be considered [for linking personal information from different systems and databases]." Also in the Glossary (p 13) it defines a persistent identifier as "an identifier which will
remain the same regardless of where the identifier is located, for example, one which is used in several independent databases”. And quite clearly the UCRN number is such a persistent identifier. For related FAQ information provided by the Improvement Service explains that the UCRN number “identifies a person born in Scotland uniquely” and that it “stays with the Scottish citizen from birth to death”. There could hardly be a better example of a ‘persistent identifier’ than this.

The proposals document (para 7, p 5) also states: “The UCRN is an anonymous number [and] contains no personal or identifiable information”, as if this might in some way invalidate the claim that it is a persistent identifier. However, a plain unique serial number can be a persistent identifier if it is a ‘cradle-to-grave’ personal number which is used to interlink records in separate databases.

2.2 Avoiding creating centralised databases of personal information

The ‘Principles’ document states (para 4.2, p 9): “Organisations should seek to avoid creating large centralised databases of people’s personal information. People’s personal data should not be acquired and aggregated in a single place but maintained in separate data stores relevant to their specific business purpose.” But the NHSCR National Identity Register is such a ‘large centralised database’ at the very heart of the scheme, and so its use is entirely against the agreed ‘Principles’. The proposals document provides no explanation for why this fundamental principle is being transgressed. This is extremely serious, as the principle fundamentally undermines any system design which employs a National Identity Register at its heart.

Conclusion: The current use of the UCRN number and the National Identity Register are in direct conflict with the Scottish Government’s Identity Management and Privacy Principles guidelines. It would therefore be prudent for all members of the government’s expert panel selected to draw up the ‘Principles’ document to be asked to examine the NIR-centred and UCRN-centred design features of this scheme, and decide whether they are - or are not - in line with the Principles as agreed.

3. Data security and ‘the honeypot effect’

Hardly anything is said within the proposals (or indeed elsewhere) about how the overall system is designed so as to guarantee data security. In an age of cybercrime and widespread hacking this must be considered to be a serious deficiency. And so, in particular, it is absolutely vital to ask whether a system with a National Identity Register at its very heart can ever be a safe and reliable system.

One of the members of the aforementioned expert panel was Jerry Fishenden, formerly national technology officer for Microsoft UK. At the time when the design of the UK identity card system was being heavily scrutinised (in 2005), Fishenden said:

“As no computer system is ever 100 per cent secure ... putting a comprehensive set of personal data in one place produces a honeypot effect - a highly attractive and richly rewarding target for criminals.”

This comment is obviously directly relevant to any systems design which places a vast NIR Register of personal information at its heart - and so is relevant to the present system being considered. And in his remarks, Fishenden is implicitly predicting that the NHSCR NIR is likely to be subject to cyber attacks from hackers worldwide.

One of the main triggers for setting up the Scottish Government’s Identity Management and Privacy Principles guidelines was the extreme embarrassment caused to HMRC when (in 2007) two CDs carrying records for 25 million individuals and more than seven million families went missing in transit:

The SNP Scottish Government (in 2009) was so determined that it would suffer no such embarrassment, that it sensibly brought together its expert panel to discuss the issues and draw up its ‘Principles’ guidelines. Unfortunately now, with its insistence on having a policy based around an NIR Register, it seems to be forgetting the sound advice it has been given, and so is putting the confidentiality of all Scottish citizens in grave danger.

So given that the NHSCR NIR is to be placed on the internet and made readily accessible to thousands of people, how long will it be before criminal hackers are breaking in and stealing the key identifying information - and thence the identities - of countless individuals? And given that the NHSCR NIR contains UCRN numbers, this essentially provides hackers with ‘skeleton keys’, providing ready access to other hackable national/local databases which use the UCRN: NHS, local authority (library, council tax, ...) etc.

Also the government would be prudent to face up the fact that the entire NHSCR NIR database could be copied and made available to criminals and foreign powers worldwide. For even the US National Security Agency, with all its wealth of security expertise, was not clever enough to avoid a vast quantity of its ‘top secret’ information being syphoned off and publicised. In its case by a single trusted ‘insider’, Edward Snowden.

So it has to be asked, what is the Scottish Government’s recovery plan if/when a copy of its NHSCR NIR is taken by a hacker, thereby compromising everyone’s identity and other confidential information? Perhaps to create from scratch a new ‘clean’ NHSCR NIR, getting everyone to change their names and dates of birth? This would obviously, of course, be quite ludicrous, but in fact it only serves to point up the fact that the creation of a centralised NHSCR NIR introduces ‘impossible to deal with’ vulnerabilities. For it means that if ever the NIR is copied it will leave every Scottish citizen’s identity and information compromised.

Conclusion: The only reliable solution available is quite clear - you must insist on not setting up a honeypot National Identity Register in the first place.

4. The identity assurance alternative

Fortunately, the verification of people’s identities, for example, to confirm their right to certain entitlements, does not depend on having a National Identity Register. Other much safer, privacy-friendly alternatives are available.
Thus, for example, the UK Government, having abolished ID cards and the UK NIR in 2010, has sought to replace them by a rather more enlightened ‘identity assurance’ system. And crucially this does not require the use of an NIR, with all its inherent privacy and security vulnerabilities. Full details can be found here. https://gds.blog.gov.uk/2014/01/23/what-is-identity-assurance/

An obvious benefit of this approach is that, given the absence of UCRN numbers, “other mechanisms, such as matching, should be used” when it is wished “to link personal information from different systems and databases”, making them fully consistent with the ‘Principles’ document (para 4.6, p 9).

5. Data privacy and Article 8 of the Human Rights Act

Any system based on the use of a centralised National Identity Register and integral unique personal identifiers (like the UCRN) has serious security vulnerabilities, as described above in Section 3.

But likewise such a system, implicitly providing direct linkages between an individual’s separate records in separate database, could very easily fall foul of Article 8 of the Human Rights Act 1998, viz:

“Everyone has the right to respect for his private and family life, his home and his correspondence.”


There can clearly be little privacy for the individual in a situation where the totality of the records accessible through the NHSCR NIR are potentially available to all civil servants with access to the system. And this problem is exacerbated, given that the NHSCR NIR is likely to become a honeypot for cyberattacks by hackers located anywhere in the world. Unfortunately, in addition, it is well known that those who have permission to access such voluminous databases can be bribed, blackmailed and otherwise coerced into locating and disclosing people’s confidential information.

A much more reliable, secure and simple solution is to abolish the NHSCR NIR-centred system, and replace it by strictly autonomous, compartmentalised databases. This is common in banking systems, where, for example, visa credit and visa debit accounts are maintained entirely separately, so that if one becomes compromised, this will not lead automatically to the compromising of the other.

To date I have been unable to locate a Privacy Impact Assessment for the proposed updated NHSCR NIR. This should certainly be made available for inspection before further comment can be provided.

6. My responses to the four consultation questions

Consultation Question 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?
NO

I am not convinced that this approach will ensure the accuracy of the data held. It seems rather haphazard and dubious in its effectiveness when compared with the routine formal registration methods used widely for obtaining UK passports, driving licences and bank accounts.

So the ‘proper solution’, as might be recommended by computing specialists would be to introduce a formal registration procedure, to be regularly repeated, say every five years. This should guarantee that the data is maintained at near 100% accuracy. The downside is that such national registration, presumably mandatory, would be seen as threatening to people’s privacy. And it is indeed not permitted in Germany for this reason. Likewise, the more accurate the register, the greater is the honeypot effect to cyber criminals (see Section 3 above).

However, an even better solution to the problem of data inaccuracy and identity verification is to use a privacy-friendly identity assurance alternative, as described above in Section 4.

Consultation Question 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?

NO

In the first place, the use of a large centralised national identity database introduces such huge data security risks (see Section 3 above) that the payback would have to be equally huge to adopt this design. And to minimise the security risks, you would be strongly advised not to place the database on the internet and make it readily available to over 100 organisations; instead you would place it offline and locate it in an isolated and heavily protected place.

The benefit listed, viz. tracing people, seems trivial when weighted against the huge security risks. And, of course, there are the huge privacy risks. For example, how can you ‘extend the current ability to trace persons’, without increasing the risk to those who, for whatever reason, would prefer not to be easily traced? This would include, for example, those wives who are trying to keep their addresses secret from aggressive partners.

There are similar concerns regarding using the system to trace people for NHS payments. These were the views stated recently by Dr Peter Bennie, Chair, BMA Scotland:

“The confidentiality of medical records, and the trust this engenders, is a cornerstone of the doctor-patient relationship.
Sharing confidential health information with the government for the identification of income tax payers (Mail) would seriously undermine this trust with the result that patients may feel reluctant to seek medical help from their doctor.

Given that there is such a strong public interest in maintaining patients' trust in a confidential health service, the Scottish Government must consider other means, outside of the health service, to identify tax payers."
(Scottish Daily Mail - letters, 13 Feb. 15)

Finally, after the revelations of Edward Snowden regarding the blanket surveillance of all our personal communications by the National Security Agency and GCHQ, the last thing that most people would want to hear is that the Scottish Government and their local council are also joining in with their own intrusive, blanket surveillance. So a plan to 'extend the current ability to trace persons' would obviously not be welcomed by the majority of people.

Consultation Question 3. In order to allow citizens to make use of 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 - There are no additional service providers who I feel should be included.

The use of a single point of entry, viz. myaccount, to a multitude of online services represents very poor security design. For once cyber criminals have got hold of a citizen's logon details, they then have free access to all the services and associated information. In a different context, it is as dangerous as foolishly using the same password for many different services: online shopping, one's bank, phone company, etc. For once one of the logins becomes compromised, they all become compromised. So it's far better to use different passwords for each service, and sensible people always do this as a matter of course.

As indicated above in Section 5, it is for the same reason that banks provide you with different accounts (and access cards) for visa credit cards and visa debit cards. So if one account (and card) becomes compromised, the other does not.

Therefore, increasing the number of service providers linked to myaccount (or to a National Entitlement Card) will only exacerbate the already significant security problems, and so this proposal should be abandoned. The most secure kind of systems design is based on a principle of modularisation or compartmentalisation, helping to limit damage to as small a domain as possible. So such a principle, commonly referred to as 'not putting all of your eggs into one basket', should be adopted here instead of the myaccount single entry point approach.

Consultation Question 4. Do you consider that the proposals set out in paragraph 18 are an effective method to identify Scottish Tax payers?
According to the two Improvement Service's diagrams in the Appendix and at:
http://www.jwelford.demon.co.uk/snec/JimKinneydiagrams.pdf

there are plans to link the 'National Citizen Account' database (essentially the NHSCR NIR), through a 'Government Gateway', not only to HMRC, but also to other UK services, such as DVLA and DWP. This would represent a massive extension of the data-sharing policy and introducing huge potential privacy and security implications for the citizen.

It is therefore obvious that the proposal to go ahead with the HMRC linkage policy, should be abandoned for the time being, and returned to only after the larger policy implications have been fully debated at and agreed by the Scottish Parliament - and indeed presented to the Scottish people to test the general popularity of this idea with them.

Finally, at a time when hopes for Scottish independence are in many people's minds, it seems to be extremely curious to be designing systems around such linkages. Continued data-sharing compartmentalisation (of Scotland and rUK systems) would therefore seem to be the most prudent and cost-effective approach, at least for the immediate future.

Dr John Welford

24 February 2015

Appendix

The two enclosed systems diagrams were produced by the Improvement Service in March 2008. I happened to discover them by chance on the web, but they are no longer accessible on the Improvement Service website. I have therefore now stored copies here:
http://www.jwelford.demon.co.uk/snec/JimKinneydiagrams.pdf
Efficient Government

Customer First

Jim Kinney – Programme Director
18 March 2008
Citizen Account Links

National Citizen Account
- Username
- Password
- UPRIN
- UCNIN
- Registered postal address
- Forename
- Surname
- Date of Birth
- Gender

My Services
- DVLA
- Income Tax Self-Assessment
- Reassert Prescriptions
- GP Appointment
- Council Tax
- Benefits
- Planning Application
- Environmental

Secure Authentication

Government Gateway
- Client Gateway ID
- Client Data

DVLA Services
- Driving Licence Assessment

NHS
- Patient Identifier
- Patient Record Details
- etc.

Repeat Prescription
- GP Appointment

Card Management System
- UCRN
- UPRIN
- Card Number
- Entitlements
- Applications
- Electronic Purse
- etc.

Local Authority
Citizen Account
- Telephone Number
- Email Address
- Account Status
- Preferred Language
- Preferred Contact Type
- Service Enrolment 1
- Service Enrolment 2
- etc.

Entitlement Card
- Council Tax
- Benefit Details
- Planning Application Details
- Order Refund

is.
improvement service