



Dame Fiona Caldicott

c/o Department of Health, London

For historical reference purposes only

Date 31 August 2016

The Scottish Government response to the National Data Guardian (England) Review of Data Security, Consent and Opt-Outs

Dear Dame Fiona

Firstly, I would like to thank you on behalf of The Scottish Government for your huge personal commitment and contribution to improving Information Governance in health and social care over the last two decades. This is a complex and often emotive area, and getting the balance wrong between information sharing and security can undermine public trust. As you will be aware Scotland followed the recommendations of the first Review back in 1997 and appointed a network of Caldicott Guardians, who are still very active in Scotland's health boards and play a vital role in safe guarding patient confidentiality and enabling appropriate information sharing to be undertaken respectfully and securely. Caldicott Guardians also take seriously their role in maintaining the confidentiality of patient information after death. Two of the Guardians represent Scotland on the UK Council of Caldicott Guardians.

Your second review in 2013 was commissioned specifically for The Department of Health (England), so our response focussed only on areas of common concern right across the UK (and indeed internationally) such as patient access to data via portals, how to make information sharing work across health and social care organisations and the addition of the new Caldicott Principle. In your latest review we have taken the same approach, and provide feed-back only on how your proposals for consent and data security may or may not work in Scotland. We have an interest in the operation of NHS Digital (formerly HSCIC), NHS

England and the Health Research Agency where they impact on our ability to provide prevention, treatment and care, and enable patients to be confident about the security of their data when they participate in research.

1) Consent models

At the outset it needs to be acknowledged that this is a highly complex and sometimes confusing area for both clinicians and patients. For decades it has been common to use the term 'implied consent' in health for example (even though it actually has no legal basis) and we agree that there does now need to be a fuller public discussion around this area before The Scottish Government can be categorical. We should also add that the legislative framework and organisational structures are different in Scotland.

We do need to be careful that any consent model does not make it more difficult to provide care and we are minded to consider taking a different path from the opt out arrangements that you have provisionally proposed for England.

So much has changed in the development of eHealth and informatics over the last decade with significantly more data processing that has to happen in order to provide direct care and in support of safe, effective care. Terms such as 'secondary purposes' are now obsolete. Patients expect clinical, professional and scientific staff to be involved in quality improvement, education, training and research. Patients expect their anonymised data to be reflected in the performance information displayed at ward or team level (e.g. healthcare associated information, improvements in patient safety etc.) and recognise that this requires authorised people to access their data in order to highlight success as well as problems. Patients expect to be asked about education and training and research and consent where identifiable data is being shared.

We all have a duty to inform the patients far more about what is happening at the front-line in GP practices and in hospitals, as well as all the other functions which they may not see in the background, but offering consent opt-outs on data processing essential for delivering high quality care and core tasks (ranging from billing, administration, bench-marking, audits, screening, patient safety programmes, regulatory investigations of professional conduct, evaluations of clinical outcomes, statistics etc.) is disruptive, costly and can reduce quality and equity of care.

This is because opt outs are not distributed randomly in the population, they are a sign of specific health needs not being addressed or lack of trust that the privacy or confidentiality will be maintained. The resultant bias provides poorer quality information for shared decision

making and the complicated process required can also be confusing to patients, particularly those with cognitive impairment or fluctuating capacity whose engagement in decision making we wish to enhance, not limit.

The direction of travel in Data Protection law is for explicit consent to be obtained where appropriate and for the subject to be very clear on what data is processed and for what purposes.¹ It is necessary for the NHS, given its unique complexity to summarise its processing activities in fair processing notices and to explain this (e.g. on GP registration forms, on patient online portals and elsewhere).

In Scotland, however, the decision about collection and sharing of information is primarily a clinical one; data is not shared without the patient agreeing to participate in a clinical process. The decision to limit the information provided to others, therefore, is part of the clinical process agreed with the patient. We are working with patient groups to agree respectful forms of words that provide sufficient clinical information for safe care but respect the right and identities of patients (including transgender) regardless of legal status. We also have arrangements in place to safeguard those whose identities need to be protected for other reasons.

The need to maintain public trust can lead the NHS to apply an opt out in very special circumstances such as the implementation of SPIRE (see below).

2) Scottish Primary Care Information Resource (SPIRE)

In Scotland, SPIRE is an initiative that will take data extracts from GP practice systems and the data will be used initially by the practices themselves for internal reviews and quality review purposes. Following a public information campaign it will be used for future NHSS public health, quality improvement and planning clinical care. Following successful piloting at Health Board level, data will also be made available for approved research projects. The patient data will be de-identified prior to leaving the GP practice, pseudonyms will be applied for data linkage purposes and robust information governance scrutiny introduced over how the data is to be used by projects. As a further safe-guard it was decided that an opt out should be offered to patients and be respected. There are two reasons for this. Firstly, this is pioneering work and it will be the first time that certain data will be extracted from GP practices to the professional team at NHS National Services Scotland (which provides analytical services).² GPs as Data Controllers quite reasonably wanted a way of being able

¹ The NHS like many other public bodies in the UK does not rely on consent in order to make its data processing lawful.

² The NHS (Scotland) Act 1978 as updated by the provisions in the Public Bodies (Joint Working) (Scotland) Act 2014, which establishes Integrated Joint Boards, provides for its role.

to respect the views of patients who did not want their data to be extracted until such times as the whole process has matured. It must also be said that the issues surrounding the launch and then suspension of Care.Data for England has created misunderstandings in Scotland as well. It should be stressed that these opt out arrangements for SPIRE are exceptional. Since the establishment of the NHS in Scotland comprehensive data as required for the provision of effective care at patient and population level has been extracted from health board services care contexts to NSS without provision for opt out. Why would you offer a data processing opt out for what are long established normal processes backed by the provisions of the Data Protection Act and Statistics Act, a requirement of Good Medical Practice and/or overriding public interest tested by IG committees? Patients do have a right to object to any data processing, but if this cannot be respected then it is important that the reasons are explained.³

3) Public Benefit and Privacy Panel for NHSS

There are some areas of data processing which can be considered additional to NHSS direct care and essential activities which support good care, such as health research. It is already a long standing position in Scotland that explicit consent should be obtained for any identifiable data used in this way. The Public Benefit and Privacy Panel has been set up for NHS boards in Scotland. It includes members of the public, Caldicott Guardians, researchers, security experts and others. The Panel scrutinises requests for the use of identifiable and de-identified data. It was set up in May 2015 to act on behalf of the Chief Executive Officers of all of the Boards in NHSS and apply a more consistent and transparent approach to scrutinising requests for NHSS data. Assessors use agreed proportionate governance criteria and core principles/precedents will develop over time informed by public opinion and engagement.

We agree entirely with your views expressed in the 2013 Review that de-identified data should be the norm, not just for research, and limit the transfer of identifiable data. We have already nationally accredited two university Safe Havens as platforms able to hold de-identified data in addition to the Board-level assurance for local 'safe havens'. We are confident that the robust governance structures now in place in Scotland mean that public interest decisions can be made without consent opt outs for de-identified data. Other sectors are beginning to follow the same model, and increasing data linkage with non-health data will

³ The NHS Constitution does make clear that patients can object to the processing of data for non-direct care purposes, but there is no absolute right to refuse. If the objection cannot be respected, then the organisation has to inform the patient of the reasons why including any statutory basis. Although NHSS is not within scope of this Constitution, Scotland does follow the above process.

mean that wider governance structures will be set up that satisfy the Data Controllers in housing, education, justice sectors etc. As well as being unnecessary from an ethical and legal point of view, it would be extremely difficult to maintain a regime of allowing opt outs for de-identified data sets for research. The cost, effort and complexity of changing legacy ICT systems would be significant, the quality of data impaired and the resultant research findings unsound as a consequence of systematic bias. When a request from a research project or clinical audit to use NHSS data has undergone robust scrutiny and has been approved, there is a duty for all concerned to make sure that the data is as complete as possible if we in the NHS are to gain the full benefit of that research and better clinical decision making.

4) Improving public perception of research

We accept that there is still a great deal of public unease around the use of health data (whether de-identified or not) for research purposes. One of the key challenges for us is to better explain what is meant by 'research'. Focus groups have shown that those patients who may be hostile to the idea of their data used outside NHSS, change their mind when they are told that the work is undertaken by respected organisations such as universities on a not-for-profit basis and that each project has to go through a rigorous scrutiny process. At the moment the number of requests to use data from purely commercial companies is very small indeed, and even then such projects are invariably collaboration with the universities and NHSS (and identifiable data does not enter the commercial sector). There are robust governance processes in place where agents of a pharmaceutical company are acting in a regulatory capacity to protect the safety of patients in a clinical trial.

We believe that the way forward is to be clearer upfront with patients about the scope and complexity of data flows in a modern healthcare setting and ensure that the explicit consent provided at GP registration, at referral (which encompasses activities that happen in the delivery of safe, effective care) and to be clear about the standards of governance and scrutiny that are in place. We would also give a categorical commitment not to use identifiable data⁴ for research without explicit consent, to offer and respect any opt out in exceptional cases such as SPIRE where there is substantially new data processing and an extra degree of trust is required. Finally, in Scotland we give a categorical commitment that patient-originated data will never be sold (only cost recovery in certain circumstances to pay for resources used to prepare, maintain, de-identify and tabulate the data on ICT platforms).

⁴ Data being identified by a trained, authorised person at the earliest possible stage. We plan to develop a 'levels of privacy' model aligned to the NHSS 'green', 'amber' 'red' approach.

In parallel with this, there needs to be greater public awareness of the robust governance structures such as the Public Benefit and Privacy Panel who carry out a public interest test on behalf of the Data Controllers and by proxy on behalf of all patients.

5) Data Security Standards and ‘tool-kits’

We share your concerns in regard to data security in the NHS, and the tougher measures we must put in place to keep up with both the external threats and the internal risks that affect the availability of services. For too long there has perhaps been a false sense of security that the NHS would not be in the front line of cyber-attacks because of the care we provide to everyone regardless of who they are. But much of the malware circulating for example does not discriminate between organisations and sadly personal health data now has a commercial value to criminals.

NHSS stopped using the IG Tool-kit that was developed in England in 2011. We took the view that although the concept of having a dedicated team checking the returns made by organisations and doing some central assurance was laudable, the amount of effort involved did not lead to the outcomes we wanted. Too often the approach worked in favour of the large organisations that had the time and money to generate the evidence of compliance in the form of written policies. And a satisfactory return for an organisation did not necessarily mean that adequate thought had gone into the specific data flows, that should be brokered and captured in information sharing agreements.

NHSS took the view in 2011 that scarce IG resource would be better spent on better procurement and contractual security clauses, on information risk assessment on specific projects, on audit, inspection, incident reporting, on improving the ICT network (SWAN) and on overcoming the perceived or actual obstacles to information sharing. To this end we have launched the Information Sharing Tool-Kit, which is a package of resources to help practitioners negotiate and then document how and when they wish to conduct information sharing. In a sense it turns the concept of the IG Tool-kit on its head, and makes clear that the emphasis should be on enabling the sharing of information for some specific use cases rather than checking an organisation’s overall IG/security maturity.

6) NHSS Information Security Policy Framework

The abandonment of IG Tool-kit in Scotland should not be seen as a lessening of information security in NHSS organisations. In 2015 we launched the NHSS Information Security Policy Framework which is closely aligned to the International Standard ISO-27001. You mention in your report that adherence to this standard was perhaps a bit ambitious for Trusts in England

and that use of Cyber Essentials developed by UK central government may be a better starting point. We take the view that although gaining formal certification to ISO-27001 is not easily achievable, it is important that Boards do work incrementally towards the standard and put in place an information security management system and the 114 control types. As part of the NHSS Information Security Policy Framework/ISO Standard Boards need to put together their security objectives for the year and have a Senior Information Risk Owner review progress at Executive Board level to complement the work of the existing Caldicott Guardian. Cyber Essentials and other initiatives should be commended, but it needs to be clear that NHS organisations are highly complex organisations employing hundreds or thousands of staff which need the full range of security controls and not just a sub-set that mitigate the cyber risks relating to external human attacks. We must not forget that by far the biggest security risks and risks to patients are still those relating to internal malfunctions that impact on the availability of services. This is why we made clear in our significant incident reporting policy (launched in 2014) that we needed to consider any major or critical incident that impacted on availability and integrity, not just those associated with misconduct of individual staff that may impact on confidentiality that tend to be focus of media attention.

7) Security and audit

Even with the launch of the cross-sector Information Sharing Tool-kit and the NHSS Information Security Policy Framework, there is far more that needs to be done in NHSS; and in particular finding better ways to measure progress over time. NHSS and partner organisations may have developed the right policies and guidance for example, but how can you be sure that they are actually working?

Your proposal to link more formally the work of the Care Quality Commission in England to reporting on security and other IG matters to the Data Guardian is important.

Although NHSS does not have a Data Guardian, we are actively looking to make a formal link between the auditing Boards with the central teams in The Scottish Government which are tasked with recording significant information security and other patient safety incidents. We need to build up new two-way relationships with auditors - who to date have had a relatively low awareness of information security - so that they are briefed on any Caldicott or IG issues prior to conducting an audit, and in turn for the Caldicott Guardian in HIS to alert their counterparts and relevant heads of Information Governance of HIS findings. The growing reliance on eHealth for business continuity means that failings in information security can have a real impact on patient safety.

We measure this impact on a sliding scale of 1 to 5 (from Negligible to Extreme) in the significant incident reporting policy and have published a common risk assessment template for boards to use to assess risk. At the same time we define the sensitivity of patient and corporate information as 'green', 'amber' and 'red' in order to inform the controls and handling of that data.

8) Public consultation and legislation

Scotland does have its own legislative framework, though in regard to health it could be argued that NHSS has to date relied far more on the provisions of the UK-wide Data Protection Act, rather than on sector specific statute law to enable information sharing (e.g. Scotland does not have an equivalent of the NHS Act and its section 251). The UK-wide Digital Economy Bill, as it currently stands, does not include health and social care. This exclusion does not in itself prevent the NHS in any of the four nations carrying out the information sharing it already does, but there is now a debate as to whether there should be changes in legislation in the Scottish Parliament that a) reflects how data sharing has already developed over the last decade and b) provide a firmer statutory basis to discharge all the services that are anticipated in health and social care.

In legislating, a balance needs to be struck between the rights of the patient (e.g. need to review the Patient Rights Act (Scotland) 2011), and the need to share more information so that the NHSS and its care partners can do the necessary information sharing to deliver services. At the same time, such legislation will need to be within the competence of The Scottish Parliament and not conflict with Data Protection and the Human Rights Acts (reserved UK-wide).

The views of the patient are of course central. And as we frame any new legislation we will need to carry out both a comprehensive public consultation and a wider public information campaign that does far more to show how essential information sharing now is for direct care, the activities which support care and the research which ultimately benefits everyone.

I have provided a more detailed response to some specific areas in the Annex below and I hope there will be dialogue between officials in The Scottish Government eHealth division who lead on IG and security matters, and those in the Department of Health (England).

We also have many of our IG resources available on publicly available web-sites, particularly:

NHSS Information Security Policy Framework and cross-sector Information Sharing Tool-kit

<http://www.informationgovernance.scot.nhs.uk/>

Charter for Safe Havens

<http://www.gov.scot/Publications/2015/11/4783>

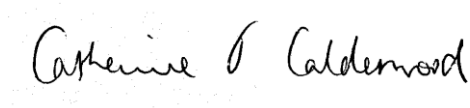
Public engagement

<http://www.farrinstitute.org/public-engagement-involvement>

<http://www.gov.scot/resource/0043/00435458.pdf>

<http://www.registerforshare.org/>

Yours Sincerely



Catherine Calderwood
Chief Medical Officer

Annex A: Scottish Government comment on specific areas of Review

This covers recommendation summary in pages 9 and 10.

Recommendation 1:

We agree. Each health Board in Scotland has now appointed a Senior Information Risk Owner, training is being undertaken and the recently launched NHSS Information Security Policy Framework makes clear the need to operate and review an information security management system. Reporting lines are important, and as part of this work Chief Executive Offices are being asked to consider how incidents and concerns are managed (dotted line from IG leads to Caldicott Guardian and SIRO) and to have a suitable distance between those in Information Assurance and the heads of ICT/eHealth.

Recommendation 2:

This is not relevant to Scotland which does not have the IG tool-kit. Emphasis has been on the new Information Sharing Tool-kit (with its resources on how to agree and document information sharing agreements and instructions), on contracts, audit, inspection, information risk assessment tailored to the data flows. In addition a certain amount of assurance work happens at organisational level for those who join the Scottish Wide Area Network (e.g. code of connection, assurance panel to consider changes and non-conformities). At Health Board level, compliance with Scottish Government guidance requires that information sharing agreements are established as standard for data flows external to NHS Scotland.

Recommendation 3:

We agree. The concept of an ICT health-check is a long-standing one, but too few organisations deploy the automated tools that report on technical vulnerabilities such as out of support software, un-approved equipment and configuration. Boards are being asked to address this work as part of the relevant control (technical vulnerability management for example) in the information security policy framework/ISO-27001.

Recommendation 4:

Cyber Essentials does have its place, particularly for external suppliers, but NHSS Boards are highly complex organisations and need to show conformance to the whole range of ISO-27001 controls not just a sub-set that relate to mitigating risk of external human attack. This is why the ISO standard is for 'information security' not 'cyber security'. In conducting a gap analysis, NHSS has found that use of SANS Institute top 20 critical controls is a useful way of checking on the sub-set of controls that help most to reduce cyber risks.

Recommendation 5:

We agree. The contract is perhaps the most important way to ensure that suppliers conform to accepted standards. This does not necessarily have to be to ISO-27001 certification or to Cyber Essentials, but it can be certain controls explicitly mentioned such as the need for staff screening, to insist in the case of software services that the product is always capable of working with the latest operating system/browser. All too often suppliers do not make adequate provision in their product road-map leading to NHS organisations being forced to maintain out-of-support software/browsers/servers and putting up with the vulnerabilities. The contract should better address this.

The forthcoming EU Data Protection Regulation, which could be maintained by UK Parliament post-Brexit, places a great deal of emphasis on the contract between the Data Controllers and the Processors and on record keeping. Given the potential of enforcement/significant fines on Processors, there will need to be clear evidence of what each party is contracted to implement by way of information security.

Recommendation 6:

We agree. Audit is a key part of the information security policy framework/ISO standard. All boards have an internal and external audit function. Since the launch of the framework, auditors are aware of how to feed back to IG committees, SIROs etc.

Recommendation 7:

We agree. Healthcare Improvement Scotland, although it does not have the same statutory basis as CQC in England, does have a rolling programme of audits and work is underway to link up its work with those central teams tasked with reporting on information security. Scotland does not have an overall Data Guardian, but the organisational structure is very different from England. Each health Board Data Controller has an executive level Senior Information Risk Owner and Caldicott Guardian, there is an overall Public Benefit and Privacy Panel whose chairman is a Non-Executive Member of a Board (currently the Board Chair of NHS Lothian), and the Chief Executive of NHSS and Chief Operating Officer are responsible for setting national policy on information security standards. In addition there is a governance structure for the use of the unique patient identifier in Scotland in routine NHS health and social care business.

Recommendation 8:

The arrangements for primary care in Scotland differ. Territorial Boards and NHS National Services Scotland provide virtually all ICT services to GP practices across Scotland so there is greater scope to obtain consistency in standards. As part of the new GP contract plans are underway to iron out any differences in the quality of ICT in practices (hardware, software, national services, network etc.) and for GP practice personnel to be fully in scope of the NHSS Information Security Policy Framework. There is a growing acceptance that in order to counter the growing cyber threats GPs will need to follow the processes and security controls laid down by the Board. In turn GPs expect that the Board provides an adequate level of ICT services.

Recommendation 9:

It is important that all significant information security incidents regardless of whether malicious or unintentional are reported up to The Scottish Government (a 1-5 scale from Negligible to Extreme has been in operation since August 2014). To date this policy has been adhered to. In the event of a Board not reporting either to SG or to the Information Commissioner, the SIRO/Chief Executive would need to justify his/her course of action. Apart from the ICO powers of enforcement/fines, the Scottish Parliament Committees can and do consider where there has been a lack of candour over significant information security issues.

Internal malicious or intentional security breaches are rare, and there already is adequate provision in the law to deal with such cases (e.g. Computer Misuse Act, Data Protection Act etc.).

It is noted that Care CERT (Computer Emergency Response Team) has been recently set up for England and joins the other well established CERTS in other sectors such as defence and central government. Scotland has set up governance structures for SWAN (Scottish Wide Area Network which includes all health boards) and now needs to consider how it deals with cross-sector cyber incidents with CERT UK.

Recommendation 10:

We agree that a lot more has to be done to explain to the public what already happens to data in a modern healthcare context. We also have to be aware of the pitfalls in confusing the normal business activities of the NHS with commercial research. It is not helpful if the NHS in any part of the UK builds up an unrealistic and unachievable expectation that patients have a right to opt out of things that they do not. It is far better to be upfront and honest and explain how care is provided and assured with examples to show how confidentiality is maintained while essential functions are undertaken and improvements in care made. Such examples might include billing (essential if for example dialysis patients are to have their human rights respected and are to go on holiday and continue their tailored programme), in addition to organising care, assuring quality and undertaking improvements in patient safety and quality and complying with the requirement to demonstrate the functioning of the NHS to the Scottish Parliament through provision of high quality statistics.

Recommendation 11:

We take a different stance to what is being provisionally proposed for England and wish to consult further. We should consider the consequences for patients being able to opt out of data processing for direct care and in support of that care within NHSS or its Data Processors contracted to it. There is adequate provision with the current Data Protection Act for this position and direction of travel in Data Protection law is for upfront explanation of data required, its purposes and to obtain explicit consent. In the context of the NHS, the range of activities is wide. The purposes are all broadly the same, which is to provide care and the administration and support of that care to current and future patients and there is a mandatory legal requirement and public interest for doing all these things. The term 'secondary purposes' is now a misnomer. As eHealth and informatics have developed, the line between direct care and other activities is increasingly blurred. Once a person is enrolled as a patient this needs to be explained. NHSS would only then consider additional opt out provisions in exceptional circumstances and for very limited data items. The roll out of SPIRE is one such case as it is a new development for GP practices, who as individual Data Controllers have signed up to the programme, to extract some data routinely and have it maintained by NHS National Services Scotland in a manner that has not happened before on this scale in primary care (in the way it has for Board specialist and community care for decades).

Recommendation 12:

The name change is a matter for NHS England/DH. Scotland does not have a direct equivalent to NHS Digital, although NHS National Services Scotland does deliver similar services ranging from ICT solutions stewardship to the central analytical and statistical work undertaken on behalf of and in partnership with all Boards.

Recommendation 13:

The ICO guidance on anonymisation is already clear here. It needs to be undertaken in such a way as to make the possibility of re-identification a remote possibility. Each Board has an Information Committee that oversees the de-identification and extraction of data to the necessary standard to local 'safe havens'. In addition there is a very mature capability at NHS National Services Scotland, that de-identifies national data sets and transfers them securely to external parties such as the newly security accredited safe havens.⁵

⁵ To date The National Safe Haven and University of Dundee have been security accredited. Others are due to follow in 2016/17. <http://www.gov.scot/Publications/2015/11/4783>

Projects that require data relating to more than one health board (or where there is a requirement for national data sets or it is high profile/contentious area) need to apply to the Public Benefit and Privacy Panel. As part of the scrutiny process, de-identification standards are considered.

In terms of overall risk, the chances of a malicious person attempting to re-identify such data (particularly from one of our accredited safe havens) is very low to remote. A person with the motivation and skills to carry out such a task would more likely attempt to obtain identifiable data from source NHSS systems. Nevertheless, the reputational impact of obtaining even a de-identified data-set is high and it is for this reason that we are security accrediting a small number of university safe havens. The Scottish Government also has security specialists who work with Boards and research teams to ensure that we remain abreast of developing threats. The acquisition of data sets by criminals and linking them up to identify people is a problem facing all sectors. There already are laws in this area which carry tough penalties. The difficulty has always been the attribution of a cyber-attack to a particular party given the long and complicated supply chains and difficulties in enforcing the law in such circumstances.

Recommendation 14:

As above.

Recommendation 15:

We agree that in the case of identifiable patient data for commercial research, individuals should provide explicit consent.

SHARE has been set up by NHS Scotland to provide a register of people interested in participating in health research. It requires explicit consent, and provides on-going information to those who agree to take part.⁶

In contrast to England, for research originating in Scotland, data is de-identified at the earliest point for internal and external use and where approved researchers require individual level data we expect key identifiers to be replaced by automatically generated meaningless numbers with the key held locally and securely.

Note: this explicit consent requirement does not apply where the project relates to the creation of clinical datasets at Health Board or national level, where the project relates to

⁶ <http://www.registerforshare.org/>

NHSS audits and other normal business. Where such data is to be used for research, research ethics approval is required and a de-identified data set created to answer specific questions. In all cases, whether it is with explicit consent or not, the governance structures at board level or the national Public Benefit and Privacy Panel are important.

Recommendation 16:

The Scottish Government is aware of this issue particularly in regard to when patients from one nation go to another in order to receive treatment. Billing is a necessary activity, and although in accordance with the Caldicott principle no more data should be used than is necessary to complete the financial aspects, it needs to be accepted that specifically trained and authorised finance professionals, who work for the NHS and are subject to its recruitment and screening processes, may need to know the basics of the condition (e.g. x procedure was carried out and overall nature of condition). It is accepted that some legacy systems are not good at masking all un-necessary data fields, but a pragmatic view needs to be taken here in order to administer the payment of services.

Recommendation 17:

We agree that more needs to be done to explain how data is used in all parts of the UK, and in particular for the research bodies to unpack the term 'research'. Research is a fundamental part of high quality clinical care and most health research is undertaken by clinical and scientific staff that are either directly employed by the NHS or University employees providing services through the honorary NHS contracts or equivalent. Most focus groups in Scotland appear to show that public concern is around the use of patient-originated data for commercial purposes. If this is the case then more needs to be done to explain that it is projects undertaken by NHS and partner organisations that are funded by governments or not-for-profit bodies who are the main receivers of NHS data. More also needs to be done to show the contribution that the commercial pharmaceutical sector play and the need for the NHS to provide high quality de-identified data if we are all to benefit from better medicines.

Recommendation 18:

This is an interesting idea. At a macro level more needs to be done by the research sector to explain what they did with the NHSS-originated data, what the project achieved and to feed-back its findings so that appropriate implementation plans can be drawn up. It is difficult to sell the public benefits of research where there is no comprehensive public engagement plan.

At a micro individual level it is not clear how this would work. Certainly for patient portals designed for specific long term conditions (there are some excellent examples such as for diabetes) more could be done to recruit people onto studies and a means to feed-back the success of the project. There are undoubtedly some groups of patients who are digitally very competent and experts on their own condition who may like such an interactive tool.

Overall, focus groups in research commissioned by Scottish Government, public panels established to guide research and those involved in research 'safe haven' development have found most patients want:

- a) knowledge that there are robust governance structures with members of the public and respected experts making decisions on their behalf;
- b) that in those exceptional cases where opt out is offered it is actually respected and
- c) that no data is being sold by NHSS.

The Farr Institute (which is a collaboration that includes Scottish Universities and NSS) is helping to address public awareness about the benefits of health informatics research.

Recommendation 19:

This submission should form part of the consultation. Although health is devolved in Scotland, there is undoubtedly a knock-on effect if England adopted a consent model which was markedly different from Scotland, Wales and Northern Ireland. There already are some key differences (Section 251 and setting aside of Common Law Confidentiality of NHS Act 2006, for example does not apply to Scotland). It should be noted that if Scotland did adopt a different consent model from England it would still be lawful in accordance with the Data Protection Act and its successor legislation.

Recommendation 20:

The current health committee structures in Scotland that will further consider how to develop the consent model and information security are The Public Benefit and Privacy Panel, The Caldicott Guardian, IG and Information Security fora and eHealth Strategy Board.

There is an increasing need to consider these issues at cross-sector strategic level given the need to share across organisations. The top level governance structure is the Scottish Government Digital Public Services Board, supported by the Data Management Board.
