Dear Dame Fiona

The second Information Governance review is most welcome and has important implications for all health and social care organisations across the UK.

We recognise in particular many of your comments about the lack of trust between NHS and local authorities due to perceived and actual differences in Information Governance, and warmly welcome the additional Caldicott principle and the presumption to share in the context of direct care. One of the lessons that has been learned from working with such a wide range of care partners in the public and private sector who handle sensitive corporate as well as patient data, is that information risks need to be taken in the round (integrity and availability risks; and not just confidentiality). And part of our NHSScotland Information Assurance Strategy, launched in 2011, is to ensure that better risk based decisions are taken where patient data is to be used in direct care and for secondary purposes such as public health and research. Scotland has a thriving medical research community and we welcome your recommendations aimed at ensuring there are adequate safeguards and maximum transparency for the public when patient data is to be used in this way.

Since your original review in 1997 a community of Caldicott Guardians has been set up in NHSScotland and I would like to put on record the enormous gratitude of the Scottish Government for the work that they do. Without them, and their expert knowledge and scrutiny, it would be much more difficult to gain the public trust required for enhanced data sharing across health, social care and researchers in allied fields.

I appreciate that this review has been commissioned by colleagues in NHS England and have therefore asked that our response to the recommendations (enclosed) deals only with the Information Governance issues that affect Scotland and the whole of the UK.

18 June 2013
Recommendation 1

People must have the fullest possible access to all the electronic care records about them, across the whole health and social care system, without charge. An audit trail that details anyone and everyone who has accessed a patient’s record should be made available in a suitable form to patients via their personal health and social care records. The Department of Health and NHS Commissioning Board should drive a clear plan for implementation to ensure this happens as soon as possible.

The Scottish Government agrees in principle that people in Scotland must have the fullest possible access to all the digital (and paper) records about them across the whole of health and social care with little or no charge. Such access helps to “support people to communicate with the NHSS, manage their own health and wellbeing, and to become more active participants in the care and services they receive” (SG eHealth Strategy 2011-2017).

However, in practice we recognise the current difficulties there are in locating, assembling, re-formatting, redacting and presenting an entire medical record to a person on demand that is held in so many formats (paper and digital) over a vast array of clinical systems. Such requests from patients create an additional workload for record managers. It is for this reason that many NHSScotland health boards and GP practices still opt to charge patients (up to a maximum amount set out in the Data Protection Act 1998) when they request to see all or part of their health records. NHSScotland takes the view that this situation is not satisfactory; and the Data Protection Act Subject Access route should be the exception to the rule. Instead, people should be routinely involved in the co-production of their records as much as possible during care. This also ensures that complex clinical information is explained to the patient (which is not possible if a digital or printed file is simply delivered to the patient). Furthermore, research has shown that patients tend to want to see particular parts of their medical record (rather than everything) and The Scottish Government is working on a number of projects that provide types of data which patients actually demand (e.g. medical summaries, allergies, medications and recent clinical correspondence relating to long-term conditions). The move towards a single digital patient record will be a slow and incremental one. And once this has been achieved it is important that there is a discussion with patients as to how and when they choose to access it (e.g. having only specific data accessible online and others only face-to-face etc.) and the technology that will allow such preferences to be captured and respected.

Similarly, in principle a patient should be able to access an audit trail that details anyone and everyone who has accessed their personal health and social care records. Such transparency can help to bolster the trust needed between patient and clinicians/professionals. But in practice, it needs to be recognised that health organisations are still a long way from this aim because of the vast number of legacy IT systems and local working practices that mean the identity of specific clinicians/professionals is not always clear on the audit logs at all times. Providing such imperfect audit trails to patients without adequate explanation and caveats (e.g. the false positives, the fact that a very wide-ranging group of medical and administrative professionals require access to patient information) could actually undermine trust. The approach of NHSScotland has been to invest in privacy breach detection tools which routinely monitor staff access to patient records. Such tools identify potentially inappropriate access in a way that is not possible with just audit logs. The aim must be to reassure patients – using every tool at our disposal such as education, training, privacy breach technology - that access is always appropriate and lawful. The request by a patient for a copy of audit logs could be viewed as a last resort, because they have not received enough reassurance from the health organisation that access has been appropriate.
Recommendation 2

For the purposes of direct care, relevant personal confidential data should be shared among the registered and regulated health and social care professionals who have a legitimate relationship with the individual.

Health and social care providers should audit their services against NICE Clinical Guideline 138, specifically against those quality statements concerned with sharing information for direct care.

The Scottish Government agrees that information should be shared among health and social care professionals who have a legitimate relationship with the individual for the purposes of direct care.

The fact that different sets of professionals work for different organisations (e.g. local government or NHS) or have different career homes (e.g. qualifications and registration in social care as opposed to medical) should not be used as a barrier to data sharing. Instead, there should always be a presumption in favour of sharing in the case of direct care.

In Scotland health and social care providers should audit their services against Healthcare Improvement Scotland (set up by Public Services Reform Act Scotland Act 2010) and in the case of local authorities, Audit Scotland.

Recommendation 3

The health and social care professional regulators must agree upon and publish the conditions under which regulated and registered professionals can rely on implied consent to share personal confidential data for direct care. Where appropriate, this should be done in consultation with the relevant Royal College. This process should be commissioned from the Professional Standards Authority.

The Scottish Government supports the view that the professional regulators need to publish the conditions under which professionals in health and social care can rely on implied consent (especially for whole records). The NHSScotland Code on Patient Confidentiality outlines the circumstances where explicit, implicit, written or un-written consent may be given in a health care setting. But it is now recognised, as a result of more integration between health and social care, that the situation is even more complex. Going for the default position that the entire health record should be shared with social care professionals involved in a person’s care has many advantages (e.g. speeding up data sharing, ensuring that the data is complete and up-to-date). But this has to be balanced with the right of the patient to withhold consent for all or part of the health care record and integrity issues (e.g. an entire health record without significant re-formating may not be intelligible to non-specialists in social care).

Recommendation 4

Direct care is provided by health and social care staff working in multi-disciplinary ‘care teams’. The Review Panel recommends that registered and regulated social workers be considered a part of the care team. Relevant information should be shared with members of the care team, when they have a legitimate relationship with the patient or service user. Providers must ensure that sharing is effective and safe. Commissioners must assure themselves on providers’ performance.

Care teams may also contain staff that are not registered with a regulatory authority and yet undertake direct care. Health and social care provider organisations must ensure that robust combinations of safeguards are put in for these staff with regard to the processing of personal confidential data.

The Scottish Government strongly agrees with the recommendation that those working in multi-disciplinary teams across health and social care should share relevant information. A traditional barrier to sharing of patient information has been a lack of trust between organisations and professions (along with a perception that Data Protection and other legislation prevents such
sharing). It is important for government to send out a clear signal that where there is a multi-disciplinary care team all the members of that team need to carry out effective data sharing for the purpose of direct care. At the same time, it is essential that prior to such sharing taking place within the team there are clear safeguards in place (e.g. contracts, data sharing agreements, Data Protection training, supervision by professionally qualified persons, capture of consent decisions etc.).

Recommendation 5

In cases when there is a breach of personal confidential data, the data controller, the individual or organisation legally responsible for the data, must give a full explanation of the cause of the breach with the remedial action being undertaken and an apology to the person whose confidentiality has been breached.

The Scottish Government takes the view that it is already routine for NHS organisations in Scotland to provide a full explanation of a data breach to those affected and detail the measures to minimise the risk of it occurring again. The use of the term ‘data breach’ rather than data loss is welcomed, and there is a case for an even wider definition as not all breaches relate directly to confidentiality risks. Many breaches for example relate to medical records which are misfiled, inadvertently destroyed or are inaccurate (and which can have clinical impacts). It is important that more of such cases are identified, acted upon and communicated to patients. The gradual process of presenting more patient information online (e.g. patient portals that show medications) could mean that patients play a greater part in being able to identify and correct problems earlier on and therefore reduce the impact of some of these types of breach.

It is also accepted that health organisations need to be better prepared (via training and processes) when handling data from third parties - which might be professionals in different sectors or family members - relating to patients. The increasing integration between health and social care, and the important role of family members/friends as carers mean that more information about a patient will come from non-medical professionals. When such information is provided (and then used to assist the patient’s care) it is important to also consider the confidentiality and other impacts on the third party. NHSScotland will consider how it can best provide better guidance on this area.

Recommendation 6

The processing of data without a legal basis, where one is required, must be reported to the board, or equivalent body of the health or social care organisation involved and dealt with as a data breach.

There should be a standard severity scale for breaches agreed across the whole of the health and social care system. The board or equivalent body of each organisation in the health and social care system must publish all such data breaches. This should be in the quality report of NHS organisations, or as part of the annual report or performance report for non-NHS organisations.

The Scottish Government notes that there is a category of data breach which might not be reported in the same way as loss of data, blagging, theft or more obvious security incidents: this is where data is shared in some way without a legal basis. The experience of NHSScotland boards is that such cases are very rare, and in fact it is far more common to have a situation (described in Chapter 3) where data is not shared because of an unfounded fear that it is not legal (when in fact there is no legal barrier under Data Protection legislation). Nevertheless, it is accepted that the massive changes which are now affecting health - with many more business partners in the private and third sector and data used by medical researchers - means there is a risk of the pendulum swinging too much in the other direction and for data to be routinely shared without a clear legal and ethical basis. The Scottish Government gives full backing to the recent ICO (Information Commissioner’s Office) guidance on Data Sharing and the need to do ‘privacy by design’ and have adequate data sharing agreements and privacy impact assessments prior to any routine sharing. And it should be noted that without the continuance of robust independent scrutiny of research requests in Scotland (i.e. usually carried out...
by Caldicott Guardians) there is a risk of Schedule 3.8.2 ‘medical purposes’ in the Data Protection Act (1998) being stretched to the point where a court of law might in the future question the legal basis for sharing.

The Scottish Government notes the current difficulties in reporting data breaches in a consistent manner across a large and complex set of health and social care organisations. This is partly because there is no standard definition of what is a notifiable data breach (i.e. the triggers to inform a health board executive, The Scottish Government etc.) and a lack of clarity over who needs to be alerted. This would explain why the statistics on breaches compiled by the ICO would differ from those in government departments. There is a need for a much more robust way of both reporting and reporting back the lessons learned.

While there may be a need for some kind of severity scale or trigger points, experience in Scotland shows that too much emphasis on scale (i.e. number of people affected by a breach) could mean that incidents relating to a small number of people are overlooked. Many data breaches relating to one person or one family for example can have significantly higher impacts (e.g. physical or mental harm) than a breach relating to a thousand people (e.g. where data missing relates only to names and addresses which can be found on the electoral roll). And while the NHS takes the view that anyone and everyone has the same right to confidentiality it is often incidents relating to high profile people that are more likely to be reported on in a very public manner (e.g. newspaper stories, Parliamentary Questions, government enquiries etc.). Similarly, there are incidents which had little or no impact but are near misses or highlight a new type of threat that should be reported at the highest level (e.g. novel form of cyber-attack which has the potential to cause significant harm in future if countermeasures are not put in place). Any standard severity scale must consider the impact on individuals’ privacy and the wider organisation and be flexible enough to take all of the factors above into account.

It is agreed that the health or social care organisation’s annual report or quality report is an appropriate place to record examples of data breaches. But it needs to be determined whether this should include literally all confirmed data breaches or those which hit a certain trigger. Whatever is published must have enough contextual information to make it useful for all people to understand the scale of the problem and how far improvements are being made. For example, simply reporting that x laptop computers were stolen over the course of 12 months does not in itself tell you very much. Instead, the public need to know whether any patient identifiable information was held on them, whether such data was encrypted (or the device itself encrypted), the likely impact on individuals’ privacy and the scale of the problem (e.g. number of devices stolen in relation to the total number of devices actually in use by the health organisation).

Recommendation 7

All organisations in the health and social care system should clearly explain to patients and the public how the personal information they collect could be used in de-identified form for research, audit, public health and other purposes. All organisations must also make clear what rights the individual has open to them, including any ability to actively dissent (i.e. withhold their consent).

The Scottish Government agrees that more should be done to explain upfront to patients how identifiable or de-identified personal information is to be used for research, public health and other purposes (e.g. via ‘fair processing notices’) and the options available to withhold their consent for one or more purposes (e.g. a patient may agree for transfers of their personal data in the interests of public health work undertaken by the NHS but not for other research purposes). It would however be impractical to undertake this communications and consent capture each and every time there is a major transfer of data relating to a high volume of patients to a ‘Safe Haven’ for example. There is a widespread misconception that such transfers of sensitive personal data can only occur where there is explicit consent from the subject. Although explicit consent is one condition (and always the preferred route), there are other ways in which processing is legal without it. Health organisations regularly rely on the ‘medical purposes’ section of the Data Protection Act in order to make processing of patient data (including identifiable patient data) for secondary purposes legal. There is
already a robust scrutiny process, comprising mainly clinically qualified Caldicott Guardians, who make this ‘public interest test’ on behalf of the Data Subjects. It is vital that this clinical oversight continues. Relying simply on communications to patients (e.g. awareness campaigns that give patients the ability to opt out of x and y secondary purposes) or relying on the research community to decide on what is legal and ethical could undermine public trust.

Recommendation 8
Consent is one way in which personal confidential data can be legally shared. In such situations people are entitled to have their consent decisions reliably recorded and available to be shared whenever appropriate, so their wishes can be respected. In this context, the Informatics Services Commissioning Group must develop or commission:

- guidance for the reliable recording in the care record of any consent decision an individual makes in relation to sharing their personal confidential data; and

- a strategy to ensure these consent decisions can be shared and provide assurance that the individual’s wishes are respected.

The Scottish Government agrees that ideally there should be a better way of capturing patient consent decisions and preferences (e.g. on the types of communication method). However, there needs to be recognition of the huge difficulty there is in achieving this aim given that Scotland, the rest of the UK (and many other developed countries) are still a long way from achieving a single Electronic Patient Record that might include such data. Typically consent decisions are captured verbally, on digital, or even paper forms, by the organisation providing the care (e.g. GP IT system) and is not easy to make this available to other organisations and kept up-to-date. We recognise that this situation, which can often mean a patient has to inform several health organisations about a change in circumstances, is not satisfactory. One option in the future may be for the CHI (Community Health Index number system which is accessible to a very wide range of organisations providing health care in Scotland) and its associated database to include consent decisions and preferences. Another is for such data to be included in key information summaries that use innovative forms of messaging and are available nationally (e.g. Emergency Care Summary or Key Information Service). Another, is for a patient portal hosted online, to enable the patient to view and update consent decisions. A holistic long-term approach needs to be taken in relation to capturing patient consent/preferences relating to wider areas of health care. For example, decisions on organ donation, resuscitation, next of kin etc. might be best captured along with decisions on data during the same care episode (or at point of registration). The Scottish Government will work towards finding a process which can be applied consistently across the country.

Recommendation 9

The rights, pledges and duties relating to patient information set out in the NHS Constitution should be extended to cover the whole health and social care system.

This recommendation relates to the Constitution for NHS England.

In Scotland the Patient Rights Act (2011) enshrines a ‘Charter of Patient Rights’ into law.

The ‘Charter of Patients Rights’ needs to be reviewed by a Scottish Minister no later than five years from the date of the charter. And any changes would no doubt reflect changes across the whole of health and social care.
Recommendation 10

The linkage of personal confidential data, which requires a legal basis, or data that has been de-identified, but still carries a high risk that it could be re-identified with reasonable effort, from more than one organisation for any purpose other than direct care should only be done in specialist, well-governed, independently scrutinised and accredited environments called ‘accredited safe havens’.

- The Health and Social Care Information Centre must detail the attributes of an accredited safe haven in their code for processing confidential information, to which all public bodies must have regard.

The Informatics Services Commissioning Group should advise the Secretary of State on granting accredited status, based on the data stewardship requirements in the Information Centre code, and subject to the publication of an independent external audit.

The Scottish Government agrees that the creation of accredited ‘safe havens’ is an important way to ensure that the risks relating to the transfer, analysis and linkage of data (whether it is identifiable or non-identifiable at any stage in the process) are minimised. NHS National Services Scotland already hosts such a safe haven, and further safe havens are being established within the four nodes of NHS Research Scotland. Although some requests for patient data are from established research organisations (who may seek large samples across a wide geographical area) there are also many more small scale projects that request a narrow range of patient data from a single GP practice for example. The challenge now is to ensure that the safe havens operate as a flexible federal network that can handle large and small scale research projects efficiently, and that privacy issues are assessed in a consistent and streamlined manner across Scotland. In addition to the NHSScotland National Caldicott Scrutiny process, the Scottish Government is considering a cross-sector National Privacy Advisory Committee as some of the most innovative research involves datasets covering different aspects of a person’s life in Scotland (i.e. health, social care, housing, environment, tax etc.).

Recommendation 11

The Information Centre’s code of practice should establish that an individual’s existing right to object to their personal confidential data being shared, and to have that objection considered, applies to both current and future disclosures irrespective of whether they are mandated or permitted by statute. Both the criteria used to assess reasonable objections and the consistent application of those criteria should be reviewed on an ongoing basis.

This recommendation relates to NHS England.

Recommendation 12

- The boards or equivalent bodies in the NHS Commissioning Board, clinical commissioning groups, Public Health England and local authorities must ensure that their organisation has due regard for information governance and adherence to its legal and statutory framework.

- An executive director at board level should be formally responsible for the organisation’s standards of practice in information governance, and its performance should be described in the annual report or equivalent document.

Boards should ensure that the organisation is competent in information governance practice, and assured of that through its risk management. This mirrors the arrangements required of provider trusts for some years.

This recommendation relates to NHS England; but has implications for Information Governance across the UK.
The Scottish Government agrees that all organisations in NHSScotland should be competent in information governance and information risk management. The Information Assurance Strategy - agreed at a national level in 2011 - has already delivered in a number of key areas.

It is also accepted that simply having qualified persons in post is not enough (e.g. IG and security leads, Caldicott Guardians, Data Protection Officers etc.); IG also needs to be represented at board level and for performance in this area to be described at a suitably high level (e.g. annual report or quality report). Information risks must be taken in the round and relate to the integrity and availability of information (not just confidentiality) and to both corporate and patient information. Simply having a Director of Public Health (who may also be a Caldicott Guardian) or Director of IT (who may have IG within their portfolio) might not provide the board executive with visibility of the full range of information risks. For this reason some organisations, such as special health boards (e.g. Scottish Ambulance Service) have appointed SIROs (Senior Information Risk Owners) who can look across the whole information risk landscape and take responsibility for it. Chief Executives, in conjunction with The Scottish Government, will consider how IG can be best represented at board level.

Recommendation 13

The Secretary of State for Health should commission a task and finish group including but not limited to the Department of Health, Public Health England, Healthwatch England, providers and the Information Centre to determine whether the information governance issues in registries and public health functions outside health protection and cancer should be covered by specific health service regulations.

This recommendation relates only to NHS England.

Recommendation 14

Regulatory, professional and educational bodies should ensure that:

- information governance, and especially best practice on appropriate sharing, is a core competency of undergraduate training; and

- information governance, appropriate sharing, sound record keeping and the importance of data quality are part of continuous professional development and are assessed as part of any professional revalidation process.

The Scottish Government takes the view that it is already commonplace for basic information governance to be part of the training/curriculum for people about to work for NHSScotland (and as an employee there is board-level training, an array of materials offered by NHS Education for Scotland and through professional bodies). The key question is how far this training is up-to-date and well-tailored to meet the new type of challenge facing health care professionals? A person graduating from a nursing college today for example needs to be equipped with the skills to work in a multi-disciplinary health care environment (e.g. involving social workers who are part and parcel of the team), to have the confidence to make sensible risk based decisions on information sharing (not just the risk based decisions that they are trained to make in medicine), to understand the risks relating to mobile and eHealth devices that may be used when out in the community and the importance of information and records management: i.e. if data is not captured correctly with due consideration to local records policies then it may not be accessible or useful for the rest of its life-cycle (and a higher risk of data breach). NHS Education for Scotland (NES) is at the vanguard here and has recently produced a range of eLearning packages.

The report makes some specific points about the capability of personnel working in Information Governance and the need for regular training of Caldicott Guardians. The Scottish Government agrees that apart from giving IG visibility at the top table (recommendation 12) the IG personnel need to be professionally qualified and of suitable grade. It should be noted however, that there can be no ‘one size fits all’ approach here as territorial and special health boards in Scotland have varying organisational structures that have grown up over decades. There are often sound local reasons why
an IG Lead might be of a particular grade, might fill the role on a part-time basis in a small organisation or report to a different team leader (e.g. Head of IT or Head of Finance) than a counterpart in a neighbouring board. What is more important is the overall outcome: that the personnel are professionally qualified, receive regular in-job training and are equipped to take a more risk based approach to information management. Without this, the IG function will continue to be perceived in some quarters as a ‘blocker’ to progress (rather than as an enabler to the business).

**Recommendation 15**

The Department of Health should recommend that all organisations within the health and social care system which process personal confidential data, including but not limited to local authorities and social care providers as well as telephony and other virtual service providers, appoint a Caldicott Guardian and any information governance leaders required, and assure themselves of their continuous professional development.

Since the original Caldicott Review in 1997, a community of Caldicott Guardians has grown up across all health boards in Scotland. Their contribution has been extremely valuable, and The Scottish Government would like to take the opportunity to put on record its gratitude and continuing support for the work that they do.

The Scottish Government notes that one way to support this group is to ensure that tailored training is provided for both new Caldicott Guardians as well as professional development for existing ones. NHSScotland does have foundation and advanced training materials and will consider how it can work with NHS Education for Scotland (NES) to do more in this area (e.g. more formal mandatory training).

Careful consideration will be given to the recommendation to widen the Caldicott Community to local authorities, social care providers and others. But it should be noted that one of the key strengths of the Caldicott community in Scotland is that there is a strong clinical core. It is this clinical expertise, backed up with information governance skills, that has enabled them to provide leadership and ownership in a way that would not have been possible if for example only specialists in information law had been appointed as ‘guardians’. As mentioned in recommendation 12, any argument for a Caldicott Guardian to be appointed in a wider set of organisations has to be squared with the fact that many of these non-NHS organisations such as local authorities have a more recent tradition of appointing SIROs or board-level representatives on information risk.

**Recommendation 16**

Given the number of social welfare initiatives involving the creation or use of family records, the Review Panel recommends that such initiatives should be examined in detail from the perspective of Article 8 of the Human Rights Act. The Law Commission should consider including this in its forthcoming review of the data sharing between public bodies.

The Scottish Government welcomes any clarity on how far the creation or use of family records might be viewed from the perspective of Article 8 of the Human Rights Act.

As there is no minimum age, in Data Protection or other legislation, that governs when a person can view their own record (or make decisions that may prevent others from accessing it) healthcare professionals have tended to grapple with the issue on a case by case basis. It is common for the body of case law around Gillick-competency to be cited, and on the whole health care professionals get the balance right.

But it is accepted that many of the developments in eHealth, such as the ability to present information to patients online or via messaging tools mean that many of the usual checks and balances that a professional might use when a patient is directly in front of them (e.g. confirming identity, deciding on what information can be released, and its impact on the individual and family members) are more
difficult to deploy. One emerging area of concern is where a family member deliberately or inadvertently accesses a patient’s health information because resources (e.g. home computers, mobile devices, email accounts, passwords) are shared. There is a strand of work in The Scottish Government assessing how far identity and access management policies used in other sectors (e.g. entitlement cards for transport) can be used in health-care and how far special safeguards need to be in place for children and young people.

Recommendation 17

The NHS Commissioning Board, clinical commissioning groups and local authorities must ensure that health and social care services that offer virtual consultations and/or are dependent on medical devices for biometric monitoring are conforming to best practice with regard to information governance and will do so in the future.

This recommendation has relevance to all parts of the UK.

The Scottish Government takes the view that although it is important to ensure that medical devices and biometric devices conform to best practice with regard to information governance it is often difficult to ensure that this is so without negating clinical safety standards. There is an increasing blurring of the lines between clinical medical devices (e.g. equipment attached to patients in hospitals or at home) and eHealth devices (e.g. more typically the computing and processing equipment). It is common for example to find medical devices that have circuitry, operating systems and applications akin to those standard desk-top or mobile computers, and yet industry and international standards relating to medical equipment – essential to ensure patient safety – assume a rather ‘hermetically sealed environment’. This means that any local change made to the device (e.g. to mitigate the risk of Internet-originated malware spreading to it) can mean the device ‘kite-mark’ or other standard is compromised. This is an area which can only be addressed at an EU/international level. The Scottish Government recognises the trend to security accredit entire business processes rather than focus just on particular medical devices, as most data breaches relate to failures in process (e.g. a person using a device in an unintended way) rather than technical security or the configuration of the devices.

A related area, addressed in the review, is the challenge of managing confidentiality and integrity risks, when devices are used outside a controlled clinical environment (e.g. tele-health equipment at home). Receiving data direct from the patient, or from a third party care provider, does create a range of trust, integrity and ownership issues. For example, if a person inputs data about themselves onto an online patient portal service set up by a third party provider, and then subsequently chooses to transfer all or part of this data to a professional in the NHS or social care then how will the data be interpreted, and will it be trusted? Will the patient-originated data then be appended (e.g. as a note) or incorporated into the formal health record in some way? How will the patient consent to this and would there be an audit trail which shows this complete journey (i.e. from its capture as ‘patient owned’ data, its digital transfer to the NHS, interpretation, amendment by a clinician and incorporation into the formal record used by everyone involved in the person’s direct care). There are as yet no clear answers to all of these issues; but it is vital that we gain clarity on them prior to rolling out the home-based and person-centred eHealth applications as part of mainstream services. The Scottish Government wants people to communicate with the NHSS and become more active participants in the care and services they receive. In order to achieve this strategic aim, the services on offer such as messaging, self-service data capture online or read-only access to medical summaries, need to be upfront and transparent about the risks (e.g. outage of service or cyber-attack), the responsibilities (i.e. of the patient, third party provider and NHS), the practical alternatives for persons with special needs and finally the options for patients to ‘opt out’.
Recommendation 18

The Department of Health and the Department for Education should jointly commission a task and finish group to develop and implement a single approach to recording information about ‘the unborn’ to enable integrated, safe and effective care through the optimum appropriate data sharing between health and social care professionals.

This recommendation relates to England.

The Scottish Government is discussing this issue as part of its Getting it Right for Every Child programme (GIRFEC).

Recommendation 19

All health and social care organisations must publish in a prominent and accessible form:

- a description of the personal confidential data they disclose;
- a description of the de-identified data they disclose on a limited basis;
- who the disclosure is to; and
- the purpose of the disclosure.

The Scottish Government agrees that the requirements under the Data Protection Act (such as formal notification and privacy notices) are a starting point rather than an end point for transparency. It is vital that health and social care organisations are open and upfront about the personal data that is collected and disclosed as part of day-to-day direct care and where it is legally disclosed (for example in de-identified formats) to other parties for other purposes (e.g. public health and research). The formal ways in which this can be achieved will be considered (e.g. making public data sharing agreements, annual report etc.) as well as the way in which such openness can be part of normal care discussions with the patient.

The Scottish Government recognises that given the increasing integration with health and social care there is a need for greater consistency in how Information Governance is organised (and a shared understanding of what this should encompass). The term ‘IG’ has a particular meaning in the UK healthcare sector, and it should not be assumed that this framework can be simply adopted by all its non-NHS partner organisations. Some non-NHS organisations for example have in more recent years placed far more emphasis on information risk management in the round (whereas there is a widespread perception that IG in health has placed too much emphasis on confidentiality at the expense of dealing with the information availability and integrity issues). And many organisations place more emphasis on the exploitation of information assets (how it is re-used and shared for research) rather than the safeguarding of it. The NHS would benefit from learning from some of these other approaches.

The value and applicability of the IG Toolkit concept (as developed in NHS England) is currently being assessed in NHSScotland. There is a concern, echoed by the Caldicott2 team, that the considerable effort involved in creating and maintaining self-assessment toolkits (and the returns from hundreds of organisations which are then generated) does not always lead to hard evidence showing improvements over time. Scotland is in the early stages of procuring a Scottish Wide Area Network (SWAN) which is expected to be used by a wide range of health, social care and other public sector organisations. There may be an opportunity to ensure that those connecting to such an IT network have an agreed level of Information Governance (in addition of course to the specific data-sharing agreements). It is still to be determined whether this IG foundation is best achieved by a toolkit-maturity model or some other method.
Recommendation 20

The Department of Health should lead the development and implementation of a standard template that all health and social care organisations can use when creating data controller to data controller data sharing agreements. The template should ensure that agreements meet legal requirements and require minimum resources to implement.

This recommendation is most relevant to NHS England and its legislation (e.g. section 251 NHS Act 2006).

It should be noted that although the above legislation does not apply to Scotland, the UK Data Protection Act (1998) does set out the conditions for processing of sensitive personal data. There are circumstances where patient data transferred and processed for the purposes of ‘medical purposes’ other than direct care and is: a) identifiable (or the ‘grey’ area of de-identified patient data that can be re-identified at some point during the research life-cycle) and b) processed without explicit consent (because this is not practicable). The decision to process identifiable (or re-identifiable) sensitive personal data without explicit consent – and in effect to act on behalf of patients and in the wide public interest - must be taken with great care, by responsible persons (i.e. Caldicott Guardians) after appropriate scrutiny. For example, a sample of identifiable data may be taken for the purposes of public health protection (‘preventative medicine’) or ‘medical research’. However, as per recommendation 10, the preference should always be for the data to be de-identified and held in accredited ‘safe havens’.

In the case of sharing for the purposes of direct care, it is now routine for NHSScotland boards and partner bodies to have Data Sharing Agreements. The Scottish Government will seek to try and standardise these as much as possible.

Recommendation 21

The Health and Social Care Information Centre’s Code of Practice for processing personal confidential data should adopt the standards and good practice guidance contained within this report.

Recommendation 22 (section 13.3)

The information governance advisory board to the Informatics Services Commissioning Group should ensure that the health and social care system adopts a single set of terms and definitions relating to information governance that both staff and the public can understand. These terms and definitions should begin with those set out in this document. All education, guidance and documents should use this terminology.

Recommendation 23 (section 13.3)

The health and social care system requires effective regulation to ensure the safe, effective, appropriate and legal sharing of personal confidential data. This process should be balanced and proportionate and utilise the existing and proposed duties within the health and social care system in England. The three minimum components of such a system would include:

• a Memorandum of Understanding between the CQC and the ICO;
• an annual data sharing report by the CQC and the ICO; and
• an action plan agreed through the Informatics Services Commissioning Group on any remedial actions necessary to improve the situation shown to be deteriorating in the CQC-led annual ‘data sharing’ report.
Recommendation 24 (section 14.1)

The Review Panel recommends that the Secretary of State publicly supports the redress activities proposed by this review and promulgates actions to ensure that they are delivered.

Recommendations 21, 22, 23, and 24 relate to NHS England.

Recommendation 25

The Review Panel recommends that the revised Caldicott principles should be adopted and promulgated throughout the health and social care system.

The Scottish Government takes the view that the Caldicott principles have stood the test of time and fully endorses the updating and addition of the seventh principle (the duty to share as well as the duty to protect). It will seek to promulgate them across the Scottish health and social care system.

Recommendation 26

The Secretary of State for Health should maintain oversight of the recommendations from the Information Governance Review and should publish an assessment of the implementation of those recommendations within 12 months of the publication of the review’s final report.

Relates to NHS England.

In Scotland the Information Assurance Strategy, launched in 2011, is reviewed on an annual basis and there is already oversight from the NHSScotland eHealth Strategy Board.

Yours Sincerely

HARRY BURNS

cc: Department for Health (England)