

Data Sharing Review

Richard Thomas and Dr Mark Walport

Consultation paper on the use and sharing of personal information in the public and private sector

List of questions for response

We would welcome responses to the following questions set out in this consultation paper. Please follow the question order as set out in the consultation paper, leaving a blank response box for any questions not answered.

Please email your completed form to contact@datasharingreview.gsi.gov.uk

Alternatively you can send a hard copy response to:

Data Sharing Review Secretariat
5.26 Steel House
11 Tothill Street
London
SW1H 9LJ

Thank you.

Section 1: Background

Question 1.

Comments:

This document is a consolidated response to the consultation from various departments and programmes within the Scottish Government

Corporate Analytical Services

The Scottish Government is interested in information sharing for operational and statistical purposes. Access to administrative data about individuals and businesses would improve the quality of statistics available to policy makers and enable assessment of the impact of policy and interactions between issues such as education, crime and employment

Analytical Services (Education) collects a wide range of Education and Social Work data from schools and local authorities through the **ScotXed partnership**. The data is mainly about children and young people and staff. The ScotXed partnership operates across the Scottish Education community and facilitates the secure, efficient and effective electronic data exchanges. Partners include Her Majesty's Inspectorate of Education (HMIE), Scottish Qualifications Authority (SQA), all Local Authorities (LAs), Careers Scotland as well as a

range of other organisations.

The data collected by ScotXed is validated and anonymised before the data is shared with 'analytical' colleagues within the Scottish Government. This effectively means that they receive a reduced and less disclosive dataset from which analytical products are produced.

Examples of 'analytical' products include annual statistics published by the Scottish Government on exclusion and attendance at schools, teacher and pupil numbers. Analytical products also contribute to the evidence base for policy development and making within the Scottish Government. We comply with the National Statistics Code of Practice.

Scottish Government **Health Directorates** develop policy for Scottish NHS Boards to help facilitate the Scottish Government's aspirations and commitments in the delivery of healthcare. These include:

- to provide patient-focused services,
- to move away from reactive to anticipatory care,
- to work and share information with other relevant public authorities (e.g. local authority)
- to provide, efficiently, the services relevant to the individual patient/service-user.
- Access (whether electronic or manual) by the right public sector worker, to the right information, at the point and time of need is integral to delivering on these commitments.

The types of information involved includes, in terms of DPA, both personal and sensitive personal data, stored electronically, in 'accessible records' (viz health records) and in 'relevant filing systems', and used, within Scottish NHS Boards and organisations, primarily for medical purposes (DPA Schedule 3 para 8)

In addition, the high-level remit of the Scottish Government's **eCare Programme** is to deliver technology change and support business change for the delivery of a number of Scottish Government policy priorities. The current scope of the Programme is set at:

- **Sharing Assessments:** Sharing electronic single shared assessment (SSA) for all community care groups in all 14 DSP geographies
- **Child Protection:** the implementation of mechanisms to deliver child protection messaging (CPM) to Social Work and Education in all the DSP Local Authorities and many functions within Health, including all out of hours health practitioners
- **Getting it Right for Every Child (GIRFEC):** defining the data and technical standards required to support the developing integrated children's agenda.

The **eCare Framework** is a cohesive set of technology standards, architectures, infrastructure and software designed to provide public sector agencies and their technology partners with a single strategic approach to enable secure multi-agency information sharing. The Framework provides the capability to address the technical barriers and costs to data sharing by agreeing a standard technical architecture. The framework allows for multi-agency data exchanges through a fully supported technical implementation and shared service.

The data sharing model is 'federated', i.e. information is retained by individual agencies and only disclosed to the framework where there is a need for multi-agency involvement. Information is shared only with the explicit consent of the service user, except where a duty of care overrides the need for that consent to be obtained (e.g. child protection). It is an approach recently publicly supported by the Information Commissioner's Office.

The Scottish Government also sponsors the **Customer First programme** which has been developed in partnership with all 32 Scottish local authorities and managed with the support of the Convention of Scottish Local Authorities (COSLA) and the Society of Local Authority Chief Executives in Scotland (SOLACE).

The programme underpins the Scottish Government's commitment to provide financial support and work in partnership with all 32 of Scotland's Councils to:

- Deliver more convenient and responsive public services;
- Encourage the take up of online (self-service) access to services;
- Ensure that at least 75% of core services requests can be dealt with at the first point of contact.

To help ensure citizens get all of the services that they are entitled to, Customer First is establishing a secure and sustainable national data-sharing infrastructure. This includes a citizen account and citizen entitlement status, linked to an address gazetteer. The account is only enabled with the informed consent of the citizen and secure business processes ensure that only updates from an authenticated (trusted) source are able to alter the status of the account.

It is not compulsory for an individual to agree to share their personal data when applying for a Citizen Account. Where they have agreed to share their personal data, this will be limited to their name, gender, date of birth and address (or contact details such as email or telephone) and their unique citizen reference number (UCRN). There are three core purposes to the data sharing. The first, is part of a validation routine to confirm entitlement to services; the second is to provide authentication credentials to citizens (e.g. for secure access to contact centre / online services); the third, is to provide a securing messaging framework within which customers can notify a change of circumstance (such as a death notification or a change of address / contacts details).

Customer First and the development of the eCare Framework initiatives help support the delivery, through distinct business processes, of services to citizens and improved data sharing. While Customer First deals, in the main, with access to general services and provides a secure framework for customers to notify basic changes to their personal data, the eCare Framework is being developed for the sharing of more sensitive personal data.

ISCJIS - Integration of Scottish Criminal Justice Information Systems – this is a programme of work to facilitate electronic communication between the various Scottish Criminal Justice Organisations (SCJOs) so that agreed information can be passed electronically from one criminal justice organisation to another saving repeated data entry, increasing speed and improving quality while maintaining confidentiality. The programme is a joint initiative by the major criminal justice agencies ie Police, Courts, Crown Office etc.

The flow of information between the criminal justice organisations in Scotland is complicated but the principal information exchange has been developed which enables criminal case information in Scotland to be transferred electronically between agencies making the criminal justice system more efficient and effective. All organisations have agreed data standards (in 1996) for the information to be passed between them.

Section 2: Scope of personal information sharing, including benefits, barriers and risks of data sharing and data protection

Question 2.

Comments:

Corporate Analytical Services

Sharing data for statistical purposes would enable better policy making whilst reducing the burdens on businesses and individuals in responding to surveys.

Health:

Key benefits to individuals:

- Improved, and more personalised health service, which, through appropriate information being available to the appropriate health service employee, helps inform planning, clinical decision-making, and therefore, overall, an improved experience of the NHS.

Key benefits to society:

- Improved public health;
- Improved intelligence (i.e. information derived in anonymised/pseudonymised form from shared information) for use by service planners and policy-makers to plan improvements to services.
- In relation to vulnerable people and children, the public interest and society more generally is served by these groups receiving safe, appropriate and humane care. improved and more personalised health

eCare

Outcomes to Citizens:

- Reduction in referral times (for eCare-supported multi-agency activity)
- Quicker access to resources and services
- Increased protection for vulnerable citizens (in receipt of eCare-supported multi-agency interventions)
- Increased involvement in care process

Practitioner related benefits:

- Less duplication
- Easier access to information

- Better informed, decision-making
- Simpler workload management

Agency related benefits:

- Fewer process resources, increased service resources
- Better planning and management information
- Increase cross-agency reporting capability
- Supports business process re-engineering

Customer First

Individuals

A Citizen Account will provide a single point of contact for all council services (over time), and allow councils to deliver them more quickly and efficiently. It will enable the customer to choose how and when they wish to communicate with their local council.

Where an individual agrees to share their data it will enable the following:

- name and/or address changes will be shared strictly within the public sector, to avoid correspondence and documentation being sent to the wrong name or to the wrong address.
- if someone dies, the death notification will be shared with other public service providers. This will help reduce the possibility of causing embarrassment and distress to family members by sending bills/letters to the deceased person.
- if an individual moves to another Scottish local authority area it will ensure, as far as possible, that they do not need to re-register to prove eligibility for the entitlements and services they currently receive.
- If an individual has proven their eligibility for a service and the same proof is required for another service, every effort will be made to automatically offer them the additional service without them having to apply or provide the details again.

Local Authorities

- Entitlement to service can be more easily established through a Citizen's Account.
- Single source of good data should reduce data maintenance effort and cost.
- Transactions should be carried out more quickly, reducing duplication and mismatches.
- Front line services staff capable of delivering a wider range of services, thereby reducing multiple staff interventions.

Other

- Enables common approach to service delivery to citizens across public sector service providers.
- Greater integration across public sector organisations
- Portability of citizen information when change of address occurs.

ScotXed

It is increasingly clear that there are advantages to be gained from sharing and exchanging data for statistical purposes. The most obvious is the potential savings in burden and compliance costs in not having to collect the same information twice. It may also be possible to use Administrative databases to report on the population faster and more regularly than conventional statistical surveys.

ISCJIS – The benefits of sharing and exchanging information electronically between criminal justice organisations has meant savings in repeated data entry, increasing speed and improving quality while maintaining confidentiality. The results make the criminal justice system more efficient and effective.

Question 3.

Comments:

Health

Key risks to individuals: if IT security and business processes, including user training and IT system design, are inadequate, this could place personal health information at greater risk from unauthorised disclosure, resulting in damage and/or distress, when it is shared.

eCare

Individuals - Risks include:

- Threats to privacy – personal data collected / shared routinely without clear purpose; data shared with more widely than originally consented to or inadequate controls over access; accidental/unintended disclosure or unauthorised access through inadequate data security; potential linkage of datasets
- Risk of fraud – routine sharing of personal information or identifiers that could provide keys for unauthorised access to financial services or sensitive personal information
- Risk of exclusion / discrimination – data being used for population profiling and service targeting without transparency of decision making

Society

- Erosion of trust between citizen's and government
- Loss of trust leads to non-participation in legitimate data sharing - loss of individual and societal benefits

Question 4.

Comments:

eCare

Most risks are associated with centralised, monolithic databases – greater security risks, less trusted, less capacity for individual judgement in relation to data sharing.

eCare approach is federated, with 14 local Data Sharing Partnerships exercising control over separate data stores and data disclosed to the common store as a result of an explicit

decision by a local practitioner, with the involvement of the data subject, locating decision-making where it belongs.

The **Customer First** National Entitlement Card system has been designed not to store details of individual transactions centrally. The central data base is very small and is for card administration, i.e. to hold basic cardholder details to deal with issuing or replacing a card. Each local authority has a separate segment of data relating to its own citizen which it controls. The information is not accessible by civil servants. Data in relation to individual services continues to be held separately by local authorities and the only people able to access an individual's data will be those who are responsible for delivering the services, whether these are concessionary fare services, library or leisure services etc.

Question 5.

Comments:

Health

The question here is often more around not the holding of information, but the appropriate sharing of, and access to, information. A number of enquiries have taken place where it has been found that poor practice in information-sharing has contributed to adverse care, and even avoidable death. In some circumstances it has been established that the relevant information was held (on file or computer and in more than one agency) but that it wasn't shared appropriately. So the challenge is that information once stored needs to be accessible, retrievable and available for appropriate sharing in the best interests of the service user and/or in pursuit of the public authority's legal obligations.

Question 6.

Comments:

Question 7.

Comments:

Corporate Analytical Services

Powers within the Statistics and Registration Services Act 2007 will facilitate data sharing for statistical purposes between Government Departments and the Statistics Board; however the Scottish Government will only benefit if data is held by the Office for National Statistics so the powers will be of limited use. An ability to share administrative data with DWP and HMRC, currently prevented by legal barriers, would enable the Scottish Government to improve its social, business and economic statistics. This would benefit policy makers by improving the evidence base available for the development and evaluation of policy, as well as those in Local Government and other bodies responsible for delivery. Improved statistics would also be of use to society as a whole to challenge and hold Government to account.

ScotXed

Scotland has a large number of national databases that would be invaluable for research if linked pan-Scotland. The research community, with many years of experience in record linkage have encountered a number of problems particularly when attempting to link data from the health sector with data from other sectors, such as education, housing and social data. Some of these have been resolved with ad hoc solutions however, many remain unresolved. Similarly, the ad hoc solutions have not been adopted as more generalised

solutions. The barriers are mainly legal.

Whilst Scotland has better routine data systems than many other countries, some countries such as Canada, Finland and Sweden have a longstanding tradition of collecting, linking and analysing routine data and may provide alternative solutions not yet tested in Scotland. Examining and learning from practice elsewhere may offer a solution.

Question 8.

Comments:

Section 3: The legal framework

Question 9.

Comments:

Health

The DPA works well as an enabling framework of information handling standards within which the use and disclosure of personal health information must take place. The importance attached to the informing of data subjects accords well with the overall direction in Scottish Government's healthcare policy of working with patients as informed partners in their care. The DP principles relating to data quality are useful drivers to improvements in record-keeping, an area in which the Scottish Public Services Ombudsman has found Scottish NHS Boards should improve.

A key weakness in the DPA in relation to healthcare uses/ sharing of personal health information in NHS Scotland arises from the narrow definition of 'medical purposes' within Schedule 3 paragraph 8. Whilst it is clear that this definition is not so narrow as to preclude vital management and planning functions, some Scottish NHS Boards have found it raises particular difficulties when attempting to fit the work of NHS-employed spiritual care advisers within the Schedule 3 paragraph 8 definition. The ICO challenged NHS guidance on spiritual care being clear that information on a person's religious affiliation is confidential information and, as chaplains are not a registered health care profession, they could not have access to such information without the explicit, informed consent of a patient. Chaplains employed by the NHS have a professional and ethical code which prevents them from either passing on information without consent or from imposing their beliefs on patients. As chaplains operate under the same constraints as the health care professionals with which they work, Scottish Ministers have welcomed their professional Association's stated intention of taking the necessary steps to see NHS chaplaincy formally recognised as a health care profession.

Another key challenge is perhaps around service improvements, and ensuring that these are consistent with both the 1st and 2nd Data Protection Principles. Where services being delivered for 'medical purposes' for which Schedule 3 paragraph 8 is being relied upon are being improved, the 'necessity' condition may, arguably, be hard to achieve; as the service improvement and associated use/disclosure of personal health information may only be desirable, and not strictly necessary. Policy-makers and service providers wish to deliver services in a manner which is beyond that which is simply necessary, but if it is impossible to meet the necessity condition, the most likely default in Schedule 3 is to paragraph 1 'explicit consent' which raises a host of further challenges. One potential solution to this would be to,

following appropriate consultation, expand the Schedule 3 paragraph 8 definition of medical purposes so that it captures not only the minimum components of safe healthcare, but also, subject to appropriate tests of proportionality, lawfulness and legitimacy (in a manner similar to Schedule 2 paragraph 6 perhaps) the principle of developing and improving the delivery of healthcare services.

Question 10.

Comments:

Health

Within NHS Scotland, compliance with the 2nd Data Protection Principle is not typically problematic. Notification to the Register of Data Controllers, supported by the provision of appropriate 'fair processing information' to patients is clearly vital to compliance.

Question 11.

Comments:

eCare

Technical and institutional barriers include:

- Perceived lack of clarity and organisational / professional support for practitioners making decisions about when to share – interaction between DPA, professional responsibilities and duty of confidentiality
- Lack of interoperable standards and tools for limiting / managing access and re-use of data at an individual level – i.e. I license use of these elements of **my** / **our** data for these purposes by these agencies

Question 12.

Comments:

eCare

- Mandatory use of PIA - at level proportionate to scale of operation – for public bodies engaging in significant new data sharing enterprise or making significant change to current
- Power of inspection for Information Commissioner.

Question 13.

Comments:

Health

The key issue that information-sharing initiatives involving personal health information in the Scottish NHS must successfully navigate is the common law duty of confidentiality. In 2001, the then Scottish Executive asked the Confidentiality and Security Advisory Group for Scotland (CSAGS) to consider the need for legislation, particularly in light of concerns about the future of epidemiological registers such as the national cancer register, and section 60 of the Health and Social Care Act in England. CSAGS advised against the need for legislation in its 2002 final report, but also recommended that the need for legislation in this area be

kept under review, a situation which has continued to this time.

Question 14.

Comments:

Question 15.

Comments:

Section 4: Consent and transparency

Question 16.

Comments:

Health

Because the vast majority of personal health information is 'sensitive personal data' in terms of DPA, any consent requirements arising from the common law duty of confidentiality and the DPA- and its other Schedule 3 requirements- are increasingly well understood.

The Emergency Care Summary project in Scotland, which involves the sharing of personal health information between GP practices and NHS Board-supplied out of hours services for the purpose of providing safe and effective out of hours care, has a two-stage approach to this area. The population of the Emergency Care Summary data repository was done on the basis of Schedule 2 para 6 and Schedule3 para 8, as well as population wide communications and the provision of an on-going opportunity to 'opt out' of the information-sharing; access to the information stored in the data repository is only done by authorised out-of-hours NHS staff after they have obtained the patient's express consent at their point of contact with the service.

The **eCare** Framework is used in cases where individual consent is required – sharing of community care Single Shared Assessment between health and social care agencies – and where there is an overriding statutory responsibility – child protection messages relating to formal child protection activity. In both cases, the requirement for consent is understood and the scope of the dataset for sharing is well defined.

Question 17.

Comments:

eCare is used where there is a requirement to share data on an individual, case-by-case basis for purposes relating to care and protection. Consent and disclosure mechanisms (including exception conditions) can be integrated with practitioner service interactions and good practice standards.

Customer First – There is no compulsion on an individual to share their personal data when applying to set up a Citizen Account. If they do agree to share their personal data this is limited to their name, gender, date of birth and address. It will also include their Unique Citizen Reference Number The data controller of an individual's personal details will continue to be their local authority and they will only use the information provided to administer local and national entitlements via the entitlement card. Citizens will be able to

see the data that is held about them on the card management system and can request a copy of this information in accordance with Data Protection principles

Question 18.

Comments:

Health

It would be useful if efforts were made by public authorities to engage with service users on: their information needs as service providers; the benefits that can arise to both service users and the wider public interest in effective information-sharing; the risks/ disbenefits that can arise (e.g. in relation to the validity of epidemiological information used for important research and planning) if information is not shared/ incomplete. This is not a trivial task, but in the absence of a contract that clarifies these matters (and as exists in commercial relationships) between public authority service users and providers, there is some work to be done.

eCare

Data Sharing Partnerships will provide a local focus for individual citizens requesting access to their shared record. In subsequent versions of the eCare technical framework we will be evaluating options for providing citizens with access to information on what data is being shared, by whom and for what purpose + direct access to appropriate elements of the shared record.

Question 19.

Comments:

eCare

The Framework code of practice provides a useful checklist for developing specific organisational policies.

PIA principles could provide a means of developing common standards and approaches to privacy across the public sector, which could help to increase public trust in data sharing. At the moment, the guidance / documentation is fairly daunting – there's a need for supporting training resources.

Section 5: Technology

Question 20.

Comments:

Health

Technology provides many opportunities for the protection of personal information that manual systems simply cannot match e.g. well defined access controls and comprehensive audit trailing. However, care needs to be taken when deciding to implement a technology that there is clarity of purpose, so that the risks of 'function creep' are diminished.

eCare

Technology, allied to standards, can provide the capacity for interoperability across disparate systems. Security and Information Assurance / risk management approaches can provide levels of protection within organisations, when staff are involved in appropriate training and development. The eCare framework sets out to provide a secure framework that can be used for personal data sharing across multiple agencies. Use of a single framework has the

potential to deliver greater consistency in approaches to security and privacy.

Currently considering the feasibility of a 'disclosure licensing' approach, analogous to Creative Commons licensing, to provide greater clarity and more effective control of data disclosure and subsequent re-use.

Question 21.

Comments:

Health

Technology changes so quickly that this may become onerous to maintain – the development of technology certainly challenged the Computer Misuse Act 1990. Perhaps developing some more detailed protection standards from the very useful starting point of the 7th Data Protection Principle, which are less likely to be overtaken by technological changes, might be a more lasting approach.

eCare

Not sure that the law should be as specific as that. In a given area there may be several competing technology standards and the landscape may change rapidly. The law could set out key principles around security and privacy and require organisations to develop policies and ensure implementation and compliance, which could be subject to audit or inspection regimes. Particular national or international standards bodies or frameworks could be referenced or recommended.

Question 22.

Comments:

Health

Privacy enhancing techniques that both minimise the risks to individuals' privacy and help to protect important research activities in the wider public interest are an important tool. Potential barriers to using them are likely around costs/ resource incurred/ time added to overall research project lifecycle

eCare

May be a case for the wider availability of standard anonymisation / pseudonymisation techniques, with appropriate accreditation regime, to address issues of public confidence. Western Australia has a data linkage body to provide both the records linkage/PET function and governance and oversight.

Section 6: International comparisons

Question 23.

Comments:

eCare

Ontario's Privacy Commissioner and support for the 'Laws of Identity' see http://www.theglobeandmail.com/servlet/story/RTGAM.20061018.gtprivacy18/BNStory/Tech_nology/home

ScotXed

The National Collaborative Research Infrastructure Strategy (NCRIS) is a programme that was announced by the Australian Government in 2004 as part of [Backing Australia's Ability – Building our Future through Science and Innovation](#).

Australia is an international leader in the scope and extent of health-related data collected at the population level. Using new technologies to integrate and link data sets, providing a valuable new resource for monitoring the health of the population and the effectiveness of health services, and for research.

The NCRIS *Population health and clinical data linkage* capability aims

- to enhance the linkage and integration of health-related data collected in Australia;
- to provide improved accessibility to these data for the research sector; and
- to support the development of improved data collection systems.

Question 24.

Comments:

ScotXed**Western Australian Data Linkage**

Data Linkage is part of the Information Management and Reporting Directorate at the Department of Health WA. The unit collaborates with the Centre for Health Services Research at the University of Western Australia, the Division of Health Sciences at Curtin University of Technology, and the Telethon Institute for Child Health Research to provide information for valuable medical and population health research. The unit was established in 1995 to develop and maintain a system of linkages connecting data about health events for individuals in WA. The unit manages the Western Australian Data Linkage System which links the core Department of Health population health data sets as well as links to external research and clinical datasets.

Question 25.

Comments:

Operations depend on access to personal identifying information derived from each of the contributing data sources, but the actual health details are stored and managed separately by delegated data custodians. These linkages are created and maintained using rigorous, internationally accepted privacy preserving protocols, probabilistic matching and extensive clerical review. Health data can be requested for ethically approved research, planning and evaluation projects which aim to improve the health of Western Australians.

Question 26.

Comments:

Section 7: Additional questions

Question 27.

Comments:

eCare

Clearer separation of citizen identification and related services/ functions from data sharing i.e. how can we ensure that the minimum amount of personal data – proportionate to the nature and assurance needs of the transaction - is used to identify / authenticate citizens.

Question 28.

Comments: