Information: to share or not to share?

Information Governance Review

Subject: Review Scope

Purpose

The purpose of this document is to set out the proposed scope of the review.

Mandate

The mandate for the Review indicates that its function is to advise the Secretary of State and make recommendations concerning the appropriate balance between the protection of personal information and the use and sharing of information to improve care:

- how information may be safely shared and better utilised to support the care of individuals and the wider population; and
- that information governance needs to enable this sharing whilst also protecting individuals’ confidentiality and respecting their wishes.

To achieve this, the Review will therefore need to consider:

- how information should be protected and held securely;
- when explicit consent for information sharing needs to be sought and recorded;
- when may consent reliably be implied and objection/active dissent recorded;
- when should de-identified\(^1\) data be used; and
- when may statutory support be relied upon and when should it be sought.

\(^1\) Definitions for key terms are covered in a separate paper
Background:

The review was developed from a recommendation by the Future Forum:

“The Government should commission a review of current information governance rules and their application, to report during 2012. The aim of the review should be to ensure that there is an appropriate balance between the protection of information and use and sharing of information to improve patient care.”

The invitation from the Secretary of State for Health to Dame Fiona Caldicott to lead the review highlighted another of the Future Forum’s recommendations namely that

“The NHS must move to using its IT systems to share data about individual patients and service users electronically - and develop a consent model that facilitates this - in the interest of high quality care”.

The information report from the Future Forum included a summary of what the forum heard on both data sharing and information governance. A list of all the recommendations from this report and proposed information governance requirements are included in Annex A.

Context:

The law provides protection for confidential and personal information but also requires that public bodies make as much information as possible available about the services they provide.

There are sometimes pressures to protect privacy and confidentiality to the detriment of individual’s care. Equally there are sometimes pressures to share information without due regard to informing individuals, seeking their consent, or ensuring the information governance protections are adequate.

---

2 NHS Future Forum Summary report – second phase, 10.01.2012, page 15
3 NHS Future Forum Summary report – second phase, 10.01.2012, page 15
5 Sections 1 & 19 of the Freedom of Information Act
Government policy is that public bodies should publish as much information as possible, generated in the course of service provision and about its services as possible. The Protection of Freedoms Act 2010-2012\textsuperscript{6} also makes provision for data to be published in reusable form wherever feasible\textsuperscript{7}.

The Cabinet Office has set out plans to make more data available, as part of the Government’s transparency agenda as a means of generating business for the UK. It has recently published the Open Data White Paper: Unleashing the Potential\textsuperscript{8} in which it provides more details of the proposals for data sharing across government agencies.

Department of Health Policy colleagues worked with the Cabinet Office to ensure that the Department took an active role in the development of this cross-Government work. Department of Health colleagues have been liaising with the Review team in this matter.

**Content of Scope:**

The scope of the review will include information relating to both living and deceased persons. Geographically, the Review relates to Information governance in England but the scope of the Review will consider disclosures both to support cross-border care provision for individuals and other uses. The scope will also include issues related to offshore processing and transfers outside the European Economic Area. In particular, it will also consider the interface between the public and independent sectors in relation to the use of patient and service user information and to onward disclosures for other purposes in relation to consideration of the legal basis for disclosure, and IG assurances to satisfy IG obligations of dislooser.

The scope includes information held in paper records and held electronically. This encompasses both patient and service user records, and other databases, data held in medical devices and stored in telemedicine and other systems.

---

\textsuperscript{6} http://services.parliament.uk/bills/2010-12/protectionoffreedoms.html

\textsuperscript{7} Clause 102 of the Protection of Freedoms Bill

\textsuperscript{8} http://www.cabinetoffice.gov.uk/resource-library/opem-data-white-paper-unleashing-potential
The parameters indicated by the letter of invitation from the Secretary of State had indicated that the scope of the review should cover the “health and care system”\(^9\). It is important therefore to consider the organisational structures that constitute the health and care system. The Review considers that the scope of the health and care system, includes public health, social care and research, but may include other aspects of care.

The Health and Social Care System formally includes the Department of Health itself, its executive agencies and the ‘arms length bodies’ as well as the commissioned health and social care service providers in England, so the organisations and the staff involved include:

**Primarily data providers\(^{10}\)**

1. Local Authorities
2. Registered health care providers
3. Registered social care providers

**Primarily data recipients**

4. Department of Health
5. NHS Commissioning Board\(^{11}\)
6. Public Health England
7. Care Quality Commission
8. Monitor
9. National Institute for Health and Clinical Excellence\(^{13}\)
10. Information Centre for Health and Social Care
11. Health Education England
12. Health Research Authority
13. Professional regulatory bodies.

---

\(^9\) Secretary of State for Health letter.

\(^{10}\) These organisations will also receive (share) personal data for operational purposes

\(^{11}\) Will also be a significant provider of data, either primarily collected by that organisations or by others
However, because the review is dealing with patient and service user information, the organisational scope is beyond the official health and care system and involves all generators and users of patient and social care service information. It therefore also includes:

14. academic researchers in universities
15. Royal Colleges in relation to professional training
16. data management and analysis companies contracted as data processors
17. “information intermediaries”\textsuperscript{12} with access to patient and service user data
18. industry, for example pharmaceutical, medical devices, data management and analysis companies, seeking to access “person-level” patient and service user data for their own purposes
19. The police and other government agencies and public bodies.

Aspects the review will consider:

1) Legal bases for processing including when consent is needed

As indicated, ensuring that the processing of identifiable information has a secure basis in law is the primary motivation for the review. This involves consideration of both current and future purposes and disclosures of personal data in health and social care. It also entails considering the legal basis on which activities are currently undertaken. Where these do not have a secure basis in law, it will identify what would be the most appropriate means of providing each purpose or disclosure with a secure basis in law.

The legal bases for processing are:

1. De-identifying the information so that it is no longer personal information and thereby is not subject to the same legal constraints;

\textsuperscript{12} Liberating the NHS: An Information Revolution Consultation Document, 18.10.2010, page 43
2. Consent;
3. Statute;
4. Public Interest - i.e. where the threshold in the public interest test can be met. The public interest test\(^{13}\) involves a balancing of the public interest in favour of disclosure with the public interest of protecting public trust in the provision of confidential services alongside the personal interests and human rights of the individual such as in maintaining their privacy. Traditionally, the public interest has a high threshold such as where there is a serious risk of harm to another individual. For this and other reasons, it should not be relied on for routine data flows.

The Review Panel will consider what is needed to support the effective de-identification of personal information\(^{14}\). This could include consideration of the risk of indirect or deductive identification of an individual where outputs are based on small numbers.

In relation to consent, there is currently no uniform approach in relation to the use of data or its recording in systems. Consideration needs to be given to: when explicit consent is needed, when it may be reliably implied, the consent process - when and how to approach individuals, what to record in systems to enable consent and the withholding and withdrawal of consent to be implemented effectively both for health and social care. This will include examining various models of consent including dynamic consent\(^{15}\).

With respect to recommending new statutory bases for processing, these should be limited to where this is necessary and other routes, i.e. using de-identified data or consent, are not feasible. Consideration should also be given to the definition of the scope of any statutory bases and what safeguards would be appropriate e.g. to ensure the processing is limited to these purposes and to prevent misuse.

---

\(^{13}\) *NHS Confidentiality Code of Practice, 7.11.2003*

\(^{14}\) A De-identification for Publication Information Standard is currently in development but as it only relates to publication, whilst useful will be of limited application.

\(^{15}\) EnCoRe ref.
Similarly, where it is thought there are reasonable grounds for using the public interest as the basis for processing, consideration will be given to defining the scope of its use. As part of this, consideration will be given to the safeguards needed to try to prevent misinterpretation of this scope, which is either more liberal or more cautious than that intended.

2) Information Governance in the new landscape

The Review will consider how to ensure information governance is embedded within the new organisational structures e.g. to reduce data breaches. This should include recommendations to maintain and improve appropriate internal information governance. For instance, to ensure there is appropriate and useful IG Training for staff in all sectors both as part of basic qualifications and ongoing training. Another example is in relation to mechanisms to improve the capacity of health and social care organisations, the voluntary sector and care homes in satisfying IG requirements particularly in relation to sensitive personal data and data sharing arrangements.

It will also include the roles and responsibilities for the new structures for information governance (i.e. their system wide responsibilities). Aspects the panel will consider are whether:

- the relevant organisations with national responsibilities have sufficient powers to undertake these effectively;
- there are gaps and how any deficiencies might be addressed; and
- any legislative change is required to strengthen the capacity of organisations to fulfil their responsibilities for information governance - this might include the need for improved legal definitions.

3) Specific Information Governance issues that affect individuals

There are a number of cross-sector information governance issues that affect individuals, which the review may also wish to give attention to, in order to assist with resolution. These include:

- Accuracy and appropriate retention of data;
• Record shielding requirements and messaging - to protect the location and contact information for children and vulnerable adults where there are safeguarding considerations.

• Whether all adopted children should be given a new NHS number or retain their NHS number when they are adopted [DoE - have not issued guidance on this].

• Sharing of data where a multi-agency response is needed e.g., where a mental health patient is missing and there may be public safety or safeguarding considerations.

• Inappropriate, unauthorised or unlawful disclosure of data;

• Sharing information with carers and recording and using information to support their needs effectively whilst also respecting both their and the patient’s confidences.

• Giving patients routine access to records raises a number of important issues of relevance, notably registration and authentication of the individual’s identity and security, information about, or provided by, other people (e.g. family members) and when parental access to children’s records should be turned off. It also introduces new risks of patients being pressurised into giving access to employers or insurers. Consideration needs to be given as to how to prevent this.

• The nature of any special challenges related to genetic data.

• The use of health information related to individuals that have died

4) Specific Information Governance issues which affect organisations:

For the above aspects, it will be important to consider:

• What changes should be considered in relation to the transition from paper to electronic records?

• The issues that arise in relation to linking data held by different organisations, in particular in relation to the legal basis for processing
and the public accountability of those organisations which have been authorised to create linkages.

- Related to this is the need for clarity about data controller arrangements, whether single, joint or in common and the requirements on data controllers contracting data processes in particular where standard contracts are used and suppliers may be accredited.

- Balancing the need to prevent deductive disclosure of identity with the need to process and present personal data according to geographical location.

- How to support effective integration of health and social care services;

- What are the boundaries of the Health and Social Care system? Where do contractors fit?

- The impact of proposals to change the EU Data Protection regime;

- The impact of societal changes in relation to autonomy and government policy in respect of shared decision-making, “no decision about me without me”.

Related to this, will be consideration of:

- What additional safeguards may be needed to provide assurance to the public, such as; independent scrutiny, certification, accreditation and audit of organisations processing significant volumes of confidential and sensitive personal data?

- What needs to be communicated to patients/service users and the public?

- Whether there are adequate means of recourse for patients and the public in relation to breaches. This would include both failures in the duty of care (e.g. through a failure to share information where it is appropriate), and breaches of confidence. Both failures in the duty of care and breaches of confidence can be significantly damaging to individuals and their relationship with services.
How can technological developments facilitate patient and service user control over their personal data?

**Key questions the review will need to consider therefore are:**

1) What needs to be done to improve the effectiveness of information sharing by clinicians, social workers and other Health and Care Services Staff to improve the care of individuals and maintain public trust in the care consultation process and its confidentiality? E.g. improving the consistency of multiple professional standards requirements and guidance documents.

2) What needs to be done to ensure that individual staff have the confidence and ability to share information appropriately in the best interests of patients and service users.

3) What needs to be done to help patients and service users more successfully exercise control over their confidential and sensitive personal information within the health and care system?

4) What needs to be done to improve the effectiveness of health and care service managers, public health specialists, clinical auditors and researchers in dealing responsibly with patient and service user information?

5) What levers can be put in place to ensure both sustained improvement in sharing information appropriately, and the public’s trust in the way the health and care system in England deals with their confidential and sensitive personal information?

6) What are the key steps necessary to enable a unified information governance framework for services, analysis and research communities within the health and care system in England that best balances their requirements with those of individual’s control of their personal information?

---

16 This includes aspects of public health that require interventions, such as screening, control of communicable diseases and environmental hazard prevention.
Annex A

Future Forum Information Report

Recommendations

Information for patients and service users

1. Information is an integral part of the service to patients and service users and the Government’s information strategy must clearly set out the responsibilities of commissioners and providers in affirming this principle.

2. Service providers must ensure that information integrates around the needs of the individual, and commissioners must ensure that they do so. The NHS Commissioning Board must lead by example in its direct commissioning of primary care and other services. It should also ensure that the levers and enablers it uses for improving quality align with this requirement.

Patient ownership of data

3. In the Chancellor’s 2011 Autumn Statement, the Government announced new measures as part of its Growth Review, which set a deadline for patient access to their online GP held records by the end of this Parliament. We support this commitment as a first step, but the information strategy must now make clear how this will be achieved, recognising that there is both a financial and time burden to GP practices and by providing meaningful help and support to them.

4. The Royal College of General Practitioners, in partnership with the British Medical Association, NHS Commissioning Board and relevant patient organisations, should be invited by the Department of Health to develop a plan that delivers the roll-out of access to patient records by 2015.

5. Switching on patient access alone is not enough, and potentially detrimental if appropriate support structures are not in place for patients so that they understand and know how to use the information. The planned roll-out of patient access to electronic records by the Government must acknowledge this and ensure that a support structure is in place, including a proper consent process.

Data sharing is vital for safety, quality and integrated care

6. The NHS must move to using its IT systems to share data about individual patients and service users electronically and develop a consent model that facilitates this - in the interests of high quality care. How this is achieved should be for individual providers to decide, but with common goals and standards. The key requirement is interoperability - IT systems
talking to each other - not a “national programme for IT”. The information strategy must clearly set out what is expected for providers of NHS services, and a challenging deadline for when this must be achieved.

7. There should be a clear contractual requirement that all organisations delivering care in the NHS or in adult and child social care have systems that allow full electronic data sharing against set standards. There can be no opt-out, regardless of whether the provider is in the NHS, private or voluntary and community sector. Commissioners must strive to ensure that this does not unfairly exclude smaller organisations, which would otherwise be accepted as “any qualified providers”.

8. The information strategy should set out how the Government will ensure the establishment of technical interoperability standards and of common standards for the structure and content of health records.

9. There must be a clear presumption in favour of hospital discharge summaries being made available to the GP and patient (or their nominated carer) at the point of discharge, and of GP referral letters being made available at the point of referral.

10. The universal adoption of the NHS number at the point of data capture and across health and social care must be turned from a long-held - and generally ignored - aspiration into a reality by 2013.

Information Governance

11. The Government should commission a review of the current information governance rules and of their application, to report during 2012. The aim of the review should be to ensure that there is an appropriate balance between the protection of patient information and the use and sharing of information to improve patient care.

Using data to drive quality

12. Using data to drive quality is a fundamental governance responsibility for health and social care organisations. The NHS Commissioning Board and Monitor must be charged with ensuring that commissioners and providers uphold this principle.

13. The kind of cultural change we want to see needs to be ‘championed’ at every level. A clinician who is responsible for organising information in support of better patient care should be identified in every organisation.

Transparency

14. The Government should set a clear deadline within the current Parliament by which all information about clinical outcomes is put in the public domain.
15. The Government should set out a clear plan for the progressive
development of quality and outcome measures to underpin the new
outcomes frameworks and support frontline clinicians in measuring for
quality improvement.

16. The information strategy should emphasise the growing importance of
patient-generated comments via all forms of social media, and the need
for the NHS and social care to learn how to use these to improve
services. It should set out a clear way forward.

**Future Forum proposed Principles that the system of Information
Governance should embody**

- Responsible data sharing is an important underpinning of safety,
  quality and continuity in the care of individuals and, through
  secondary uses such as clinical audit and research, a vital component
  of wider learning and quality improvement.

- Information governance should be seen as the enabler of
  responsible sharing and extraction of data in the interests of
  improving the care of individuals and of wider quality
  improvements.

- It is the patient’s and service-user’s data and needs to be treated
  with respect.

- There should be a normal presumption that all those individuals
  involved in the care of a patient or service user have access to the
  data about that person - with their consent.

- The implicit “deal” or “contract” between service and service-user
  needs to be made explicit.

- There should be a normal presumption that, when an individual’s
  data is used for purposes other than for the care of that individual, it
  is transmitted in an anonymised or pseudonymised form. Where there
  is a need to use identifiable data, there needs to be an information
  governance framework that controls this. This framework should be
  transparent to patients.

---

## Future Forum Recommendations: Information Governance requirements

<table>
<thead>
<tr>
<th>IG requirement</th>
<th>Source reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Shared professional record-keeping standards needed to ensure meaningful shared data and data quality of integrated records. Interoperability.</td>
<td>Information integrated around the needs of people rather than organisations. Recc 2</td>
</tr>
<tr>
<td>2. Robust audit trails of authorship, profession of author (to identify if a H or a SC record), and employer of author (data controller).</td>
<td>Individuals caring for a patient having access to records. Page 17</td>
</tr>
<tr>
<td>3. Authentication of citizen identity for secure patient /service user access to records online.</td>
<td>Patient access to their records Reccs 3 &amp; 4</td>
</tr>
<tr>
<td>4. Measures to help ensure patients not put under duress to provide access to their records to employers / family etc</td>
<td>Patient access to their records Reccs 3 &amp; 4</td>
</tr>
<tr>
<td>5. Information for patients about the nature of health records (in particular) as a contemporaneous note of: what the patient has said; what the clinician has observed; actions taken e.g. tests requested; other information in the record e.g. results of tests previously taken; and clinical opinion (the clinician’s educated guess at that time based on the information available). It should therefore be factually accurate about what happened in the consultation but not necessarily in terms of accuracy of diagnosis. Patients (and some clinicians) have a different concept of the written record as “fact” and this is where problems can arise when a patient disputes the accuracy of the record and wants information amended or removed from the record and the clinician refuses. This is also part of the source of anxiety for clinicians in giving patients routine access to their records.</td>
<td>Patient access to their records Reccs 3 &amp; 4</td>
</tr>
<tr>
<td>6. Seriously harmful and data about or from other individuals- Under the Subject Access provisions of the DPA, information deemed seriously harmful to the patient (e.g. perhaps if they were a suicide risk) and information about others, or information provided by others in confidence about the patient/service user would be redacted from the record prior to disclosure to the patient. Consideration</td>
<td>Patient access to records Reccs 3 &amp; 4</td>
</tr>
</tbody>
</table>


<p>| 7. | Information for patients about the extent of control they may exercise in relation to their records - clarity about the boundaries. | Patient “ownership”/control of data Page 14 &amp; Recc 5 |
| 8. | Interoperable consent model(s) for care and other purposes - needed to ensure consent can be effectively recorded and communicated through systems to enable implementation of the patient’s wishes. | Patient “ownership”/control of data Page 14 &amp; Recc 5 |
| 9. | De-identification standard / tools / technologies to facilitate linkage whilst protecting patient confidentiality | Aggregated, anonymised data needs to flow for purposes other than direct care. Presumption that when data used for purposes other than care it is transmitted in anonymised / pseudonymised form. |
| 10. | Data security - a people as well as a system issue, how to reduce data breaches to improve patient confidence | Data security highlighted because of breaches |
| 11. | Transaction messaging - need to move these from paper to electronic communications as quickly as possible and make available to patients. Consideration of whether insecure email (uncrypted) is more secure and therefore preferable to insecure post (i.e. not recorded delivery) in terms of communication with patient - also consent issue and how to manage more sensitive data. KP approach - message to say information available on secure portal. | Swift availability of referral letters and discharge summaries to patients and receiving clinician/service |
| 12. | NHS number is important as unique identifier for individuals both for direct care and as the root identifier for pseudonymisation. There are circumstances where it is not appropriate to use e.g. GUM clinics and IVF treatment (and legally prohibited) so need to accommodate these exceptions. There are legacy system issues with full adoption, and it is often problematic in the context of A &amp; E where the patient’s identity and therefore the | Full adoption of NHS number by 2013 |
| Correct record cannot be identified. Also issue of verification. Even once fully adopted there will remain a small number of duplications and NHS number missing records which will need to be managed. Consideration should also be given to the NHS number being legally defined as a General Identifier in DP terms. |
|-----------------|-----------------|
| <strong>13.</strong> Need to ensure that national organisations consider whether their purposes really require personal data and to undertake privacy impact assessments (reqmt of H &amp; SCA 2012). Also to ensure they use the Information Centre as an Honest Broker in obtaining and providing the data in de-identified form. |
| Concern about national bodies powers to extract PID as set out in the Act &amp; requirement that aggregated, anonymised data be used for purposes other than direct care. |
| <strong>14.</strong> Need for greater public awareness of how information is used and what controls they may exercise - lack of explicit social contract with the patient. Often more issue for health than social care. |
| Public unaware of how personal data is used and shared. Lack of explicit contract. |
| <strong>15.</strong> Need for public engagement/debate (more than a consultation exercise? Akin to debate about “presumed consent” for organ transplantation) about what the public will tolerate in relation to data sharing in different contexts and for different purposes and consent / controls /degree of flexibility in the mechanisms needed. |
| Concern about proposals to share data with independent healthcare providers and that data be included in research automatically unless the individual has opted out. |
| <strong>16.</strong> Information governance capacity in the voluntary sector - in some ways potentially better because smaller organisations and more personal relationship with clients but also many do not have highly developed IG controls. Also sharing of data in LAs can be not just SC but also Housing, Voluntary Sector and other providers. Often mistrust across sector and organisation boundaries, which may or may not be justified. Contracts and information sharing protocols / agreements can assist with this as well as joint staff training. |
| Facilitating access to information by the voluntary sector where they are providing services to individuals |
| <strong>17.</strong> IG Staff training - understanding the rules to give staff the confidence to know when to share and when not to, to know when to refer and to whom to refer queries and about documenting decisions |
| Challenge of IG is that appropriate sharing is sometimes not happening and inappropriate sharing |</p>
<table>
<thead>
<tr>
<th></th>
<th>sometimes is happening.</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.</td>
<td>Suggests there is an ongoing need for something akin to the ECC function where consent is not practicable. This needs a higher public profile however.</td>
</tr>
</tbody>
</table>