Consent and Information Governance in Cambridgeshire and Peterborough

Workshop findings

December 2016

Geoff Hinkins

Geoff.hinkins@cambridgeshire.gov.uk

Background

On 14 July, a workshop was held for Information Governance professionals, operational staff and other relevant professionals from across the health and wellbeing system in Cambridgeshire. The aim of the day was to reach a common understanding across health, social care, housing and voluntary sector organisations in Cambridgeshire and Peterborough about:

- Levels of consent required when sharing information about people who receive, or may benefit from, health and care services; and
- How to establish the legal framework for sharing to take place, ensuring that any barriers to sharing are highlighted and overcome.

Information sharing is a commonly cited barrier in providing more integrated care for people across local organisations; and has been identified as a key challenge across planning of services in Neighbourhood Teams; in making referrals between organisations; and in sharing information about who is known to different services. A particular issue across Cambridgeshire and Peterborough is the issue of the level of consent required when sharing information about individuals. Interpretations of the law and aspects of Information Governance differ across the county on whether 'explicit' consent is required in any circumstances; or whether there are circumstances in which 'implicit' consent is sufficient for information to be shared. Likewise the common law duty of confidentiality and data protection legislation and other legislation can make it confusing and complicated to share data and information. The particular circumstances in which a clear agreement on levels of consent required would be helpful include (but are not limited to):

- Early help referrals for people who are beginning to become more vulnerable;
- Case finding to identify people that are receiving services from a number of organisations and may benefit from a more co-ordinated approach;
- Case management, with a lead professional identified for each person and an agreed plan spanning all the services that they receive;
- Secondary use of data to support service planning, research and strategy
- Shared care records that bring together information held about individuals into a single system

The workshop explored many of the issues above in an effort to reach an agreed position; this report represents the summary findings of the workshop.

The Caldicott Principles

The Caldicott Principles were first described in the first Caldicott Report into the use of patient information in the NHS. They remain central to our approach to the use of people's personal information:

1. **Justify the purpose(s)**
   Every single proposed use or transfer of patient identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate guardian.
2. **Don't use patient identifiable information unless it is necessary**
   Patient identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).
3. **Use the minimum necessary patient-identifiable information**
   Where use of patient identifiable information is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.
4. **Access to patient identifiable information should be on a strict need-to-know basis**
   Only those individuals who need access to patient identifiable information should have access to it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes.
5. **Everyone with access to patient identifiable information should be aware of their** responsibilities
   Action should be taken to ensure that those handling patient identifiable information - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.
6. **Understand and comply with the law**
   Every use of patient identifiable information must be lawful. Someone in each organisation handling patient information should be responsible for ensuring that the organisation complies with legal requirements.
7. **The duty to share information can be as important as the duty to protect patient** confidentiality
   Professionals should in the patient's interest share information within this framework. Official policies should support them doing so.

Data Protection Principles

From Schedule 1 to the Data Protection Act

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –
   (a) at least one of the conditions in Schedule 2 is met, and
   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The Common Law Duty of Confidentiality:

If information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider's consent.

In practice, this means that all patient information, whether held on paper, computer, visually or audio recorded, or held in the memory of the professional, must not normally be disclosed without the consent of the patient. It is irrelevant how old the patient is or what the state of their mental health is; the duty still applies.

Three circumstances making disclosure of confidential information lawful are:

- where the individual to whom the information relates has consented;
- where disclosure is in the public interest; and
- where there is a legal duty to do so, for example a court order.

Key messages

Overall, the group agreed twelve key messages for Data Sharing – these are contained in an appendix to this report.

Most importantly there was a **broad consensus on lawfulness and willingness to share with care providers and other public services.** Our organisations recognise the benefits of sharing information; and agree that with reasonable policies in place and adequate communication, the sharing that we want to carry out is legal. We will commit to working together to ensure that appropriate sharing can take place.

Secondly, the group recognised that there is **no one size fits all approach to sharing data**. The precautions that need to be put in place will vary depending on what is being shared; who is involved; and how much data is being shared. Our approach needs to be proportionate – and importantly we should restrict what we share, **only sharing personal confidential data if it is necessary.**

As well as the specific recommendations for individual projects described in the rest of this document, there are three key pieces of work that should be taken forward by the Data Sharing Board:

1. Ensure that all organisations are signed up to the Cambridgeshire Information Sharing Framework – and have agreed a common set of clear, transparent principles on consent, information governance and the use of personal information – a common 'data processing notice'

2. These principles then need to be widely communicated to staff through ongoing training and awareness raising, and included in inductions for all staff who might have access to patient and service user data. They should be made widely available – displayed prominently on each organisation's website; displayed in offices, surgeries and care locations; and shared with new patients and service users.

3. These principles need to form the basis of a marketing campaign, making clear to patients and service users:
    a. The benefits of information sharing;
    b. How we will work together to share people's information; and
    c. How we will work together to keep people's information safe.

The remainder of this report highlights the scenarios explored during the workshop, and makes recommendations for an appropriate approach to information governance and consent in each.

Data Sharing Scenarios

Early help referral

Summary:

We want staff across the system to be able to act as 'eyes and ears' – trained to spot indications that someone is becoming more vulnerable, and to refer them to appropriate support. This includes not just clinical or social care staff, but any public or voluntary sector worker who comes into contact with the public. This might include support for staff to enable them to go beyond their core role to provide some low level interventions, where appropriate. Indicators would lead to a planned response to offer support, advice and information. Data to be shared may include the contact information necessary to allow a referral, and a brief description of the nature of the concern identified.

Suggested approach:

- The officer should tell the citizen that they think they might benefit from another service; and should either:
    - Provide information so that the citizen can refer themselves; or
    - Ask for their permission to forward their details on to another organisation. In this situation, verbal consent is acceptable – the citizen should not be required to fill in a form to record their consent. The officer should record the discussion; but this does not need to be logged centrally.
- The officer should then use an existing / agreed referral process with the individual's details.
- This applies equally to sharing information within the statutory sector and with partners in the voluntary sector.
- The officer should only share the information that is necessary for the referral to take place. Where the referral is not a formal medical referral, they should not share the individual's complete record, or details of any condition or circumstance that are not relevant to the request.
- Sharing and use of the persons details should be restricted to the purpose the consent was obtained and as outlined in the organisation's Fair Processing Notice. Where possible this should be provided to the citizen.

Multi-disciplinary team working: case finding and case management

Summary:

We want to use data from across organisations to identify patients who may benefit from the MDT case management process. This data might include medical triggers such as low mood/depression, continence/ frequent Urinary Tract Infections (UTIs), injuries caused by falls, or frequent missed medical appointments. This data will highlight people whose needs are changing over time, to indicate that they might benefit from further support in order to remain independent; and could include identification of patients by care professionals based on their contact with the patient, with a referral into the case finding process. This could be achieved, either through sharing of data from a range of organisations which is then analysed by a single system, in which case data shared would include individual details such as medical conditions and history; or by each organisation analysing their own data and only sharing information on the individuals identified as most at risk. In this case, sharing could potentially be achieved using only a personal identifier (such as an NHS number) and a proxy risk 'score' generated based on an agreed weighted algorithm.

Suggested approach:

- Explicit consent is **not required** from individuals for a single organisation to identify people at risk, as long as the data does not leave that organisation.
- However, in order to share that information with other organisations, steps must be taken to protect the person's personal confidential data.
- In order to share the information, explicit consent **will not be required** as long as the following guidelines are adhered to:
    - The data shared does not identify the person or persons that the data is attributable to. This can be done through 'pseudonymisation' (encryption) of the individual's NHS Number. This ensures that it is difficult to identify an individual if the data were to be intercepted.
    - The minimum necessary data to identify people who may benefit from case management should be shared. Data that might allow people to be identified should not be shared.
    - People's identities should only be revealed once the data has been compared between organisations – and must only be revealed for those individuals who will be offered a service.
- Once people's identities are revealed, the **next step** should be to contact them and ask for them to provide their **explicit consent** for case management. If they refuse consent, information gathered for the exercise should be disposed of safely; and their withdrawal of consent should be noted.
- When the exercise is repeated, individuals who have previously withdrawn consent should not be contacted for an agreed period.
- To formalise the approach described here, a **data processing agreement** should be drawn up between all partners contributing data (the **data controllers**). This must name the organisation receiving data as a **data processor** and provide clear guidelines for use of the data.
- Alongside this – patients should be made aware that this data processing is happening, through publicity shared in surgeries, care centres and when they come into contact with staff.

MDT proactive case management

Summary:

MDT (multi-disciplinary team) proactive case management describes an agreed approach to case management, with a lead professional identified for each person and an agreed plan spanning a range of services in health, social care and wider statutory and voluntary sector organisations. Plans will be personalised and based on the person's needs and choices. Teams will include social care staff who will be aligned to, or 'vertically integrated' with Neighbourhood Teams to ensure the appropriate person is identified as the lead professional. The benefits of MDT working will be built upon with an assumption that this is a way of working that won't always rely on a set meeting; more a team around the person mode where the relevant professionals come together. To work effectively, professionals across the MDT will need to work in an integrated way, and are likely to therefore have access to a wide range of medical and care information about individuals identified for case management.

Suggested approach:

- Put simply, **explicit consent should be sought and granted** before an individual is discussed in detail by an MDT / Neighbourhood Team.
- A request should be made by the Neighbourhood Team or MDT Coordinator. The request should make clear the benefits of case management to the individual and the positive effect that it is expected to have on their care; and should make clear what information will and will not be shared (and in particular be clear that no information from financial assessments will be shared between organisations).
- If the individual does not have capacity to consent, the request should be directed to the person that has permission to make decisions on the individual's behalf. The request should be restricted to case management and not invite a blanket refusal to share data under any circumstances.
- If consent is refused, this decision must be respected; and the decision should be recorded.

Secondary use of data

Summary:

Any use of health and care data other than directly providing care to an individual is classed as 'secondary use'. This includes (but is not limited to) healthcare planning, commissioning, public health, clinical audit and governance, benchmarking, performance improvement, medical research and national policy development. Use of data in this way is essential in planning and developing services and improving care for the population. However, precautions need to be taken to ensure that data is used appropriately.

Suggested approach:

- Personal confidential data that allows an individual to be identified **should not be shared** for secondary use.
- Data can be freely shared if it is **anonymised:** that is that all patient identifiable data has been removed.
- When individual patients need to be tracked across services provided by different organisations, it is possible to share **pseudonymised** data.
- If pseudonymised data is to be used, then a data processing agreement should be drafted and agreed between all parties to the sharing.
- At all times, the general principle of sharing the minimum data necessary should be adhered to. The data sharing agreement should define the data necessary for the exercise, and sharing should be limited to that data.

Shared care records

Summary:

A stated aim of the Data Sharing Project is for practitioners and professionals to have appropriate access to all relevant data held about a person when making decisions about their care needs.

Currently, data are recorded in a variety of different electronic systems within and across services in health, social care and other organisations. Typically it is not possible for a professional in one part of the system to see information that is held in another - so the GP might not know what the mental health team has written about a patient and vice versa; and hospital staff cannot easily view information held by social care that might be pertinent to the patient's care. Where professionals have permission to view more than one record, this generally requires them to log into more than one system – and this often results in that access being underused.

As an interim solution, in some areas, selected staff are being offered access to multiple organisations' systems in order to see information held across organisation boundaries; but it is noted that this approach is sub-optimal and introduces additional risks. A key priority for the future will be to establish a shared record, or single view, so that professionals can access data in other systems in order to make the best possible decisions and recommendations about people's health and care services. This system would require a mechanism that would either:

- Access other systems and pull data across for individual patients at the point of access;
- Pull all data held in various systems into a central system that would offer a single view of the patient's record; or
- Offer a single shared record separate from each organisation's core system that would allow information to be inputted by all services.

Suggested approach:

- Significantly more work is needed on information governance surrounding a move towards a single system containing shared records.
- The goal is to move towards a system where **implied** consent allowed the sharing of information into a central system; and **explicit** consent was used for the accessing of each individual record.
- However, this would need to be accompanied by a significant publicity campaign to ensure that that residents might reasonably expect their data to be used in this way.
- 'Patient held' solutions should be explored as an alternative – these systems allow patients to control which professionals can access their data and rely on explicit consent and patient opt-in.
- In the interim – sharing access to systems presents a useful way of sharing information. Each organisation remains responsible for their own systems, and should reach their own decisions about appropriate levels of access. However, it is recommended that:
    - Where systems are shared, this should be governed by a Memorandum of Understanding between organisations.
    - Where possible, access should be limited so that individuals that do not need to see a full record can only access the information that they need.
    - Access requests are documented; and individual access is reviewed regularly to establish whether it is still needed; and
    - Where possible, use is audited.

APPENDIX: 12 Key messages:

The following statements were agreed by participants in the workshop on the day:

1. **There is a broad consensus on lawfulness and willingness to share with care providers and other public services**

The vast majority of organisations recognise the benefits of sharing information; and agree that with reasonable policies in place and adequate communication, the sharing that we want to carry out is legal. We will commit to working together to ensure that appropriate sharing can take place

2. **The level of consent required is balanced by data volume and sensitivity**

Consent can be explicit or implicit; and our approach needs to be proportionate, based on what is being shared. We do not always need to seek explicit consent if the level of data being shared is low and not very sensitive – and if the individual might reasonably expect that we would share that information.

3. **We need a governance framework that includes all parties**

The Cambridgeshire Information Sharing Framework has signatures from the majority of public sector organisations in Cambridgeshire, but not all. We need to work to ensure that all organisations are signed up to a set of principles about how information will be used across the system.

4. **Training is needed across our organisations**

There are currently different understandings of what is possible and what is appropriate across all levels of our organisation. Training is needed to ensure that consistent messages are shared throughout our organisations

5. **We need to engage patients and service users in our discussions**

It was agreed that we would consider how best to involve patient and service user representatives in our work, to ensure our plans are informed by what citizens would reasonably expect

6. **Frontline change must be supported by timely, proportionate and accurate data**

It was agreed that access to data was necessary to support change across our services – in order to understand the effect that changes were having on our services and on demand

7. **Nothing happens without communications and branding**

We agreed that our organisations need to agree a consistent set of messages about information sharing and widely communicate these – with a clear and recognisable brand and focusing on the benefits of information sharing

8. **As well as seeking consent, we need to understand what to do when it is refused**

If we are to rely more on implicit consent, the system needs a definite way of managing the process when individuals withdraw their consent for sharing. This needs to make clear for those individuals how their services will be less coordinated as a result

9. **Organisational risks are low in terms of the Information Commissioner's Office; but high in terms of reputational damage**

The biggest risk to our organisations (assuming we have clear policies and follow them) is in reputational damage if we get this wrong.

10. **Don't use personal confidential data if you don't have to**

It was recognised that sharing anonymised or pseudonymised records is preferable to sharing personal information wherever possible.

11. **Data's role is strategic**

Data is needed to support strategic planning. Individual's information is information – data is anonymised

12. **We should explore opportunities to put people in control of their data**

People should be able to see the data held about them – and if they want to, decide who can access what.