Derby City Council

HEALTH AND WELLBEING BOARD
Thursday 16 January 2014

ITEM 13a

Report of the Director of Public Health

Caldicott 2 Review: Information - to share or not to share: The Information Governance Review

SUMMARY

1.1 In 1997, Due to concerns of how patient information was being used, the Chief Medical Officer of England commissioned a review of all patient-identifiable information passing from National Health Service (NHS) organisations in England to other NHS or non-NHS bodies. The Caldicott Review identified six principles guiding the use of patient identifiable information:

1. Justify the purpose
2. Don't use patient identifiable information unless it is absolutely necessary
3. Use the minimum necessary patient identifiable information
4. Access to patient identifiable information should be on a strict need-to-know basis
5. Everyone with access to patient identifiable information should be aware of their responsibilities
6. Understand and comply with the law.

1.2 In January 2012 the NHS Future Forum recommended a review "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". The Government accepted this recommendation and asked Dame Fiona Caldicott to carry out a review – known as Caldicott2.

1.3 The scope of Caldicott2 is wider than the review of 1997, its recommendations affecting all organisations working in the health and social care sector.

1.4 Caldicott2 reviewed and endorsed the six principles (with slight updates) of the first Caldicott review. In addition, a seventh principal "The duty to share information can be as important as the duty to protect patient confidentiality" was added.

1.5 A total of 26 recommendations were made by the Caldicott2 review. The Government made a full response to the review accepting its findings and agreeing, "…that the standards, good practice and principles contained in the Report should underpin information governance across health and social care services." (Department of Health, 2013)

1.6 Many of the Reviews recommendations have implications for the Health and Wellbeing Board and its member organisations. These include:

- People must have the fullest access to all electronic care records about them, across the whole health and social care system, without charge.
- For the purposes of direct care, personal confidential data should be shared amongst the registered and regulated health and social care professionals who have a legitimate relationship with the individual. Social workers should be considered part of the 'care team'.
- Providers must ensure that sharing of personal confidential data is effective and safe and commissioners must assure themselves on providers' performance on this.
- All organisations within the health and social care system which process personal confidential data are recommended to appoint a Caldicott Guardian and any information governance leaders required.
- Rights, pledges and duties in the NHS Constitution should be extended to cover the whole health and social care system.
- 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.
- 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.
- Linkage of personal confidential data requiring a legal basis from more than one organisation for any purpose other than direct care must be done within an 'accredited safe haven'.
- Given the number of initiatives involving the creation or use of family records, the review recommended that such initiatives should be examined in detail from the perspective of Article 8 of the Human Rights Act.

1.7 Sharing personal confidential data in relation to health protection issues such as the outbreak of infectious disease can be considered as resembling the requirement to share such information for the purpose of direct care.

The establishment of a task and finish group was recommended to determine whether the information governance issues in public health functions outside health protection and cancer should be covered by specific health service regulations.

References:

Dame Caldicott (2013) *Information - to share or not to share: The Information Governance Review*. Department of Health.

Department of Health (2013) *Information: To Share or not to Share Government Response to the Caldicott Review.* Department of Health.

The Caldicott Committee (1997) *Report on the Review of Patient-Identifiable Information*. Department of Health.

RECOMMENDATION

2.1 The Health and Wellbeing Board and its constituent member organisations adopt the revised principles set out in Caldicott2 and implement the recommendations locally as appropriate.

2.2 The Health and Wellbeing Board promotes the implementation of the expectations and commitments by local health and social care organisations as set out in the Government's response to the Caldicott2 review.

2.3 The Health and Wellbeing Board seeks appropriate assurance that any sharing or processing of personal confidential data in the delivery of its priorities is done safely and effectively and on an appropriate legal basis, for example, through statement of compliance signed by each constituent organisation and ratified by the Board.

REASONS FOR RECOMMENDATION

3.1 To ensure that the Health and Wellbeing Board and local health and social care organisations support the safe and effective sharing of personal confidential data between all those with a legitimate relationship with the individual for the purpose of their direct care and in the best interests of the patient.

3.2 To provide assurance to the Health and Wellbeing Board that local health and social care organisations are fully aware of the Caldicott2 review and are appropriately implementing its recommendations.

SUPPORTING INFORMATION

4.1 Due to concerns of how patient information was being used, in 1997 the Chief Medical Officer of England commissioned a review of all patient-identifiable information passing from National Health Service (NHS) organisations in England to other NHS or non-NHS bodies for purposes other than direct care, medical research, or where there is a statutory requirement for information. A committee was formed chaired by Dame Fiona Caldicott. The Caldicott Review identified six principles guiding the use of patient identifiable information:

1. Justify the purpose(s)
2. Don't use patient identifiable information unless it is absolutely necessary
3. Use the minimum necessary patient-identifiable information
4. Access to patient identifiable information should be on a strict need-to-know basis
5. Everyone with access to patient identifiable information should be aware of their responsibilities:
6. Understand and comply with the law

In addition, the Caldicott Review made a total of 16 recommendations. The full review, including its recommendations can be found:

http://webarchive.nationalarchives.gov.uk/20130107105354/http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_4068404.pdf

4.2 Increasingly information governance is cited as an impediment to sharing information, even when sharing would be in the patient's best interests. In January 2012 the Future Forum workstream on information recommended that a review of information governance should be commissioned. This recommendation was accepted by the Secretary of State for Health in England and asked Dame Fiona Caldicott to undertake an independent review. This review, Information – to Share or not to Share: the Information Governance Review' (Caldicott 2) was published in March 2013. The Review, whilst recognising that the six Caldicott principles remained relevant and appropriate, were updated and a seventh added. The updated Caldicott principles are:

1. Justify the purpose(s)
Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

2. Don't use personal confidential data unless it is absolutely necessary
Personal confidential data 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 personal confidential data
Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

4. Access to personal confidential data should be on a strict need-to-know basis
Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

5. Everyone with access to personal confidential data should be aware of their responsibilities
Action should be taken to ensure that those handling personal confidential data — both clinical and non-clinical staff — are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. Comply with the law
Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

6. The duty to share information can be as important as the duty to protect patient confidentiality
Health and social care professionals should have the confidence to share information

in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

4.3 Caldicott2 made 26 recommendations, these are outlined below:

People's right to access information about themselves
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.

Direct care of patients
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.

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.

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.

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.

Personal data breaches

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.

Information governance and the law

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).

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.

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.

Research

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 Group60 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.

Commissioning

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.

New and emerging technologies

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.

Data management

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.

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.

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.

System regulation and leadership

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

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
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.

Conclusions and recommendations
Recommendation 24
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.

Recommendation 25
The Review Panel recommends that the revised Caldicott principles should be adopted and promulgated throughout the 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.

4.3 The Government has made a full response, "Information:
To Share or not to Share Government Response to the Caldicott Review" (link: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251750/9731-2901141-TSO-Caldicott-Government_Response_ACCESSIBLE.PDF) to the Caldicott2 Review.

The Department of Health agreed that the standards, good practice and principles contained in the review should underpin information governance across health and social care services and that the recommendations should be implemented within the spirit intended by the review's findings.

In its response, the Department of Health sets out the expectations and commitments of relevant organisations and bodies. Those relating to: staff and workers; health and care organisations; NHS providers; and commissioners are outlined below (numbers

in brackets refer to the Review recommendation number):

Who	What
All staff and workers within the health and care system expectation	• be aware that the duty to safeguard children or vulnerable adults may mean that information should be shared, if it is in the public interest to do so, even without consent (introduction) • look at information governance best practice and how it affects their work (introduction)
All health and care organisations expectations	• examine their existing arrangements, and lead by example with their local partners to make it easier to share information (introduction) • expect that relevant personal confidential data is shared among the registered and regulated health and social care professionals who have a legitimate relationship with the individual (2) • seek advice from the ICO and refer to the HSCIC's Confidentiality Code of Practice for further advice on managing and reporting data breaches (5) • explain and apologise for every personal data breach, with appropriate action agreed to prevent recurrence (5) • 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 (7) • make clear what rights the individual has open to them, including any ability to actively dissent (7) • use the best practice contained in the HSCIC's Confidentiality Code of Practice when reviewing their information governance practices to ensure that they adhere to the required standards (12) • that social care providers use the Information Governance Toolkit (12) • appoint a Caldicott Guardian or Caldicott lead with access to appropriate training and support (15) • local authorities consider extending Caldicott Guardian arrangements to children's services (15) • strengthen their leadership on information governance (15) • ensure that the information provided to inform citizens about how their information is used does not exclude disadvantaged groups (19) • use the revised Caldicott principles in all relevant information governance material and communications (25)
Local NHS providers expectation	• audit their information sharing practices in adult NHS services against NICE Clinical Guideline 138 (2)
Local commissioners expectations	• use the NICE Quality Standard 15 in commissioning and monitoring adult NHS services (in relation to information sharing) (2) • investigate, manage, report and publish personal data breaches and ensure that commissioned bodies are investigated, managed, reported and published appropriately (6)

Who	What
	• implement appropriate arrangements in relation to information governance including the demonstration of strong leadership on information governance and adopt information governance procedures that are equivalent to those already established by healthcare providers (12)

OTHER OPTIONS CONSIDERED

5.1	No other options considered.

This report has been approved by the following officers:

Legal officer **Financial officer** **Human Resources officer** **Service Director(s)** **Other(s)**	 Derek Ward, Director of Public Health Richard Boneham, Head of Governance and Assurance

For more information contact: **Background papers:** **List of appendices:**	Alison Wynn, 01332 643106, Alison.Wynn@nhs.net. None Appendix 1 – Implications

Appendix 1

IMPLICATIONS

Financial and Value for Money

1.1 Potential financial implications should a data breach be identified and prosecuted with award of a financial penalty.

Legal

2.1 Required to hold, share and process personal confidential data in accordance with the law e.g. Data Protection Act.

Personnel

3.1 The Review concluded that health and social care professionals should have formal information governance education focused on their roles, and this should be at both undergraduate and postgraduate level. This could have implications for staff training and development.

Equalities Impact

4.1 None.

Health and Safety

5.1 None.

Environmental Sustainability

6.1 None.

Asset Management

7.1 Health and social care records must be kept in accordance with legal requirements. Information assets must be mapped and assigned to 'asset owners'.

Risk Management

8.1 Holding, sharing and processing personal confidential information must be done legally requiring robust management and assurance processes. Boards must ensure that their organisation is competent in information governance and that this is assured through its risk management processes. Failure to appropriately manage information governance risk could result in prosecution, significant fines and loss of reputation.

Corporate objectives and priorities for change

9.1 Effective and appropriate information governance is central to supporting delivery of

corporate objectives and priorities.