Information Sharing Agreement

Islington Safeguarding Adults Board
Partner Organisations

August 2015
Version 1

ISLINGTON
Information Sharing Agreement

Copyright Notification

Copyright © London Borough of Islington 2015
This document is distributed under the Creative Commons Attribution 2.5 license. This means you are free to copy, use and modify all or part of its contents for any purpose as long as you give clear credit for the original creators of the content so used. For more information please see: Creative Commons Licence

Contacts

If you need any further information about this document or any clarity about the contents of the document, please contact: Eleanor Fiske Eleanor.Fiske@islington.gov.uk

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Reason for change</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>March 2015</td>
<td>0.1</td>
<td>Introduction of Care Act 2014</td>
<td>Eleanor Fiske</td>
</tr>
<tr>
<td>March 2015</td>
<td>0.2</td>
<td>Comments from the Caldicott Guardian</td>
<td>Eleanor Fiske</td>
</tr>
<tr>
<td>April 2015</td>
<td>0.3</td>
<td>Comments from Legal Services</td>
<td>Eleanor Fiske</td>
</tr>
<tr>
<td>May 2015</td>
<td>0.4</td>
<td>Comments from Communications &amp; Policy Subgroup</td>
<td>Eleanor Fiske</td>
</tr>
<tr>
<td>May 2015</td>
<td>0.5</td>
<td>Comments from Islington Safeguarding Adults Board partners</td>
<td>Eleanor Fiske</td>
</tr>
<tr>
<td>July 2015</td>
<td>0.6</td>
<td>Approval by Islington Safeguarding Adults Board subject to amendments to Section 13.</td>
<td>Eleanor Fiske</td>
</tr>
</tbody>
</table>

Distribution:
This document has been distributed to:

<table>
<thead>
<tr>
<th>Name</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Michael Woolcott</td>
<td>Caldicott Guardian</td>
</tr>
<tr>
<td>Mary-Anne Anaradoh</td>
<td>Lawyer</td>
</tr>
<tr>
<td>Communications &amp; Policy Subgroup</td>
<td>Subgroup members</td>
</tr>
<tr>
<td>Islington Safeguarding Adults Board</td>
<td>Partner organisations and Signatories to this agreement</td>
</tr>
</tbody>
</table>
Information Sharing Agreement

Reviewing the agreement

The Agreement will be reviewed annually and subject to change dependent on any changes legislative changes and national guidance.
## Contents

<table>
<thead>
<tr>
<th></th>
<th>Purpose</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Parties to the agreement</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>Why is the information being shared?</td>
<td>5</td>
</tr>
<tr>
<td>4</td>
<td>What information is being shared</td>
<td>6</td>
</tr>
<tr>
<td>5</td>
<td>Legal justification for sharing</td>
<td>7</td>
</tr>
<tr>
<td>6</td>
<td>Has consent been gained?</td>
<td>7</td>
</tr>
<tr>
<td>7</td>
<td>How will the data be shared? (include details of data transfer)</td>
<td>7</td>
</tr>
<tr>
<td>8</td>
<td>How will the data be stored?</td>
<td>8</td>
</tr>
<tr>
<td>9</td>
<td>Security &amp; Risk Management</td>
<td>8</td>
</tr>
<tr>
<td>10</td>
<td>Who will handle the information?</td>
<td>8</td>
</tr>
<tr>
<td>11</td>
<td>How long will the information be kept?</td>
<td>9</td>
</tr>
<tr>
<td>12</td>
<td>How will the data be destroyed?</td>
<td>9</td>
</tr>
<tr>
<td>13</td>
<td>Related procedures/policies</td>
<td>9</td>
</tr>
<tr>
<td>14</td>
<td>Governance, Approval and review</td>
<td>10</td>
</tr>
<tr>
<td>15</td>
<td>Appendix 1 - The legal basis for information sharing</td>
<td>122</td>
</tr>
<tr>
<td>16</td>
<td>Appendix 2 – List of ISAB partner organisations party to this agreement</td>
<td>211</td>
</tr>
<tr>
<td>17</td>
<td>Appendix 3 – Sensitive data sets</td>
<td>233</td>
</tr>
</tbody>
</table>
Information Sharing Agreement

1. Purpose

1.1 This Information Sharing Agreement (ISA) defines the arrangements for processing data between partner organisations of the Islington Safeguarding Adults Board (ISAB). For a list of parties to this agreement see Appendix A.

1.2 This ISA sits underneath Islington Council’s overarching Information Sharing Protocol (ISP) and replaces all existing ISA approved by the Safeguarding Board. The appendices provide further information and guidance should this be needed.

1.3 This ISA is intended to meet the recommendation in paragraph 14.157 of the Care and Support Statutory Guidance that Safeguarding Adults Board partners should draw up a common agreement relating to confidentiality which sets out the principles governing the sharing of information.

2. Parties to the agreement

<table>
<thead>
<tr>
<th>Originating organisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of Organisation</td>
</tr>
<tr>
<td>Address</td>
</tr>
<tr>
<td>Address line 2</td>
</tr>
<tr>
<td>Address line 3</td>
</tr>
<tr>
<td>Postcode</td>
</tr>
</tbody>
</table>

A list of ISAB partner organisations party to this agreement is contained in Appendix 2 of this agreement.

3. Why is the information being shared?

3.1 Appropriate information sharing among partner organisations of the ISAB is essential to safeguard and promote the wellbeing of adults at risk in Islington.

3.2 In line with the Care and Support Statutory Guidance early sharing of information is key to providing an effective response where there are emerging safeguarding concerns.

3.3 ISAB partners recognise that the initial legal responsibility for personal information resides with the organisation that first created or received it – in this case being the participating Data Controllers. But if personal information is shared, the responsibility extends to the recipient in the receiving organisation, regardless of how transitory that storage of the personal information might be by the receiving organisation.
3.4 It is the expectation that staff and volunteers in ISAB partner organisations will share information to:

- safeguard adults at risk of harm
- ensure that deprivations of liberty safeguards are undertaken appropriately
- decide if there is sufficient reason not to seek consent, and seek any that is considered necessary; and
- if consent is refused or no response is received, decide whether disclosure should be made in the absence of consent
- assist the ISAB to meet its objectives as defined in its Constitution

4. What information is being shared

4.1 Personal data including demographic details, identifiers such as NHS number, address, photograph, CCTV image together with personal records, health and social care plans, safeguarding concerns and other information held by partner agencies relating to possible concerns about abuse or neglect of a person at risk of abuse or neglect.

4.2 Information held by partner agencies which may be of assistance to a safeguarding enquiry, a safeguarding adults review or a Domestic Homicide Review

4.3 Sensitive and/or personal information and data for the purposes of analysing trends in safeguarding. These may include but not be limited to:

- Information relating to training, learning and development of staff in safeguarding adults, mental capacity act, deprivations of liberty safeguards
- Information relating to partner organisations' Disclosure and Barring Service checks and implementation of Islington Safer Recruitment Guidance
- Information required to complete the Islington Safeguarding Adults Return to Department of Health

4.4 Information to enable audit, quality assurance and self-assurance of safeguarding practice, policies, procedures and arrangements of ISAB and/or individual partner agencies

4.5 Generally there is no restriction on sharing depersonalised information. However, partner organisations accept that a duty of confidence, contractual or other legal restriction may apply in certain circumstances to sharing some
Information Sharing Agreement

depersonalised information. Partner organisations must take great care when depersonalising information to ensure that an individual's identity cannot be revealed.

5. Legal justification for sharing

5.1 Section 45 of the Care Act 2014 places a duty on partner organisations and others to comply with a request from the Safeguarding Adults Board to supply information to it or to some other person specified in the request if the request is made for the purpose of enabling the Safeguarding Adults Board to exercise its functions and provided other specified conditions are met.

6. Has consent been gained?

6.1 The starting point in relation to sharing personal and/or confidential information is that practitioners will be open and honest with families and individuals about why, what, how and with whom information will or could be shared.

6.2 In line with the Caldicott Review 2013 and the Care and Support Statutory Guidance, informed consent should be obtained from the relevant individuals, but, if this is not possible and other adults are at risk of abuse or neglect, it may be necessary to override the requirement.

6.3 Where an individual lacks capacity, staff are expected to make a judgement about whether sharing the information is in their best interests or in the public interest. When considering whether disclosure is in the public interest, for example to prevent or assist in detecting a crime, the rights and interests of the individual must be taken into account. A fair balance between the public interest and the rights of the individual must be ensured.

6.4 All ISAB partner organisations must confirm that they have in place a policy that addresses consent requirements and that is monitored, and supports compliance with the Data Protection Act 1998 and the Care Act 2014.

6.5 The reasons for breaching client confidentiality must be fully recorded and clearly reference the evidence and information on which the decision is based.

7. How will the data be shared?

7.1 Wherever possible, physical data transfer will be avoided. It is preferable to 'share' data through enabling authorised others to view and update data within partner organisations' record management systems.

7.2 Where data is 'sent' electronically, this will be done through secure email systems, encrypted data and/or password protected documents.
Information Sharing Agreement

7.3 Due care will be taken in sharing paper records and the requesting and disclosing professionals will ensure that any personal or sensitive information is transferred in a secure manner.

8. How will the data be stored?

8.1 Sensitive data will be securely stored by the respective ISAB partner organisations.

8.2 Personal data will be securely stored by the respective ISAB partner organisations, and wherever possible, using access controlled case management systems to restrict the viewing of and access to an individual’s records.


9.1 All staff must use their organisations approved secure email system when emailing sensitive information. Where Health Professionals are unable to comply with their organisation’s policies regarding the safe and secure transfer of data they must ensure that a risk assessment is undertaken by their Information Security/Governance department at the earliest opportunity.

9.2 Each organisation must ensure that mechanisms are in place to address the issues of physical security, security awareness and training, security management, systems development, role based security/practitioner access levels, receiving and transfer of data and system specific security policies.

9.3 Any concerns or complaints received relating to the processing of personal data will be dealt with promptly and in accordance with the internal complaints procedures of that partner organisation and, where appropriate, may be raised with other partner organisation’s responsible manager.

Breach and Escalation Rules

9.4 Any breaches will be recorded as prescribed under Islington’s Security Incident Policy. Each organisation signed up to this agreement needs to notify the partner organisations should any breaches occur.

10. Who will handle the information?

10.1 Professionals in ISAB partner organisations and Islington Council may handle the information on a strictly need-to-know basis for the purposes set out in this agreement. Professionals must be able to justify fully the reasons for their obtaining any particular detail about an individual or any sensitive information about a partner organisation or the work of the ISAB.

10.2 Each organisation must ensure that relevant staff have the necessary level of security clearance.

V1; Aug 2015
Information Sharing Agreement

10.3 Each organisation must ensure that all relevant staff receive training, advice and ongoing support in order to be made aware, and understand the implications, of this ISA and any associated documentation.

11. How long will the information be kept?

11.1 Each ISAB partner organisation is expected to have a Records Management policy with detailed guidance on retention periods for the full range of health and social care records as well as business and corporate records that is in line with the NHS and Social Care Code of Practice and medico-legal requirements.

12. How will the information be destroyed?

12.1 Once the information has been flagged for review when the retention period ends, the relevant Manager in the relevant ISAB partner organisation will approve the deletion of the record. The ISAB partner organisation will then arrange for the case record or sensitive data and all associated files to be permanently deleted or destroyed with a complete description added to the record destruction log of when the data was deleted or destroyed.

13. Related procedures/policies

13.1 This information sharing agreement sits alongside with other inter-agency information sharing agreements in operation. It is designed to enhance existing arrangements rather than replace them.

13.2 ISAB partner organisations are expected to have robust information policies in place which apply to all staff, partner organisations, contractual third parties and agents who use facilities and equipment, or have access to, or custody of, customer or patient information or other sensitive information. Information policies should address:

- Code of Conduct for Employees
- ICT Security
- ICT User Management
- ICT Security Incidents
- Third Party Access
- ICT email
- ICT Physical Security of Information
- ICT Information Risk
- Data transport
Information Sharing Agreement

13.3 Examples of suitable information policies can be viewed by clicking on the following link: Islington ICT Policies.

14. Governance, Approval and Review

14.1 This agreement must be formally approved by the ISAB and partner organisations before any information sharing takes place.

14.2 The undersigned signatories agree with the content of this document and will ensure that the ISA and any associated documents are known and understood by all staff involved in the process.

Originating organisation

<table>
<thead>
<tr>
<th>Name</th>
<th>Role</th>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Islington Council</td>
<td>CORPORATE DIRECTOR, HOUSING + ADULT SOCIAL SERVICES</td>
<td>[Signature]</td>
<td>8/9/15</td>
</tr>
</tbody>
</table>

Partner organisation(s)

<table>
<thead>
<tr>
<th>Name</th>
<th>Role</th>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Islington Clinical Commissioning Group</td>
<td>DIRECTOR OF QUALITY &amp; INTEGRATED GOVERNANCE</td>
<td>[Signature]</td>
<td>14/9/15</td>
</tr>
<tr>
<td>Whittington Health NHS Trust</td>
<td>DIRECTOR OF NURSING</td>
<td>[Signature]</td>
<td>12/10/15</td>
</tr>
<tr>
<td>Camden and Islington Mental Health NHS Foundation Trust</td>
<td>DIRECTOR OF NURSING + PEOPLE</td>
<td>[Signature]</td>
<td>7/OCTOBER 2015</td>
</tr>
<tr>
<td>London Metropolitan Police</td>
<td>DCI PUBLIC PROTECTION</td>
<td>[Signature]</td>
<td>12/9/15</td>
</tr>
<tr>
<td>Moorfields Eye Hospital NHS Foundation Trust</td>
<td>DIRECTOR OF NURSING &amp; ALLIED HEALTH PROFESSIONS</td>
<td>[Signature]</td>
<td>24/9/2015</td>
</tr>
<tr>
<td>London Fire Brigade</td>
<td>BROUGH COMMISHER</td>
<td>[Signature]</td>
<td>24/9/2015</td>
</tr>
<tr>
<td>London Ambulance Trust</td>
<td>SEPARATE AGREEMENT TO BE DEVELOPED</td>
<td>[Signature]</td>
<td>18/9/15</td>
</tr>
<tr>
<td>Healthwatch</td>
<td>CHIEF EXECUTIVE</td>
<td>[Signature]</td>
<td>18/9/15</td>
</tr>
</tbody>
</table>
## Information Sharing Agreement

<table>
<thead>
<tr>
<th>Organization</th>
<th>Position</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>London Probation Service</td>
<td>HEAD OF NPS CAMDEN AND ISLINGTON</td>
<td>9/10/15</td>
</tr>
<tr>
<td>Community Rehabilitation Company</td>
<td>ASSISTANT CHIEF OFFICER</td>
<td>16/09/15</td>
</tr>
<tr>
<td>Single Homeless Project</td>
<td>CHIEF EXECUTIVE</td>
<td>5/09/15</td>
</tr>
<tr>
<td>Age UK</td>
<td>CHIEF EXECUTIVE</td>
<td>28/10/15</td>
</tr>
<tr>
<td>Notting Hill Housing Group</td>
<td>ASSISTANT DIRECTOR NH PATHWAYS</td>
<td>9/10/15</td>
</tr>
</tbody>
</table>
Appendix 1 - The legal basis for information sharing

Care Act 2014

Section 45 of the Care Act 2014 ("the Care Act") places a duty on partner organisations and others to comply if a SAB asks them to supply information to it or another person, provided specified conditions are met. (The SAB can only request information for the purpose of enabling or assisting it to exercise its functions. The powers of the SAB are wide; being anything the SAB believes necessary to help and protect adults at risk of harm. See Section 43(2) of the Care Act 2014 which sets out the objective of the SAB.

However, any information supplied by partner agencies or anyone else under section 45, may only be used by the SAB for the purpose of exercising its functions.

Section 81 of the Care Act also places a duty of candour on providers about failings in hospital and care settings, and section 92 creates a new offence for health and adult social care providers supplying false or misleading information which they are required to provide under a statutory provision or other legal obligation. Section 94 sets out the circumstances in which a director, manager, secretary or similar officer of a care provider is also liable to be prosecuted for the offence.

Paragraphs 14.157-161 of the Care and Support Statutory Guidance recommend that agencies should draw up a common agreement relating to confidentiality and setting out the principles governing the sharing of information, based on the welfare of the adult or other potentially affected adults. Such agreement should be consistent with the principles set out in the Caldicott Review 2013 (further detail below).

➢ Where an adult refuses to consent to information being disclosed for these purposes, then practitioners must consider whether there is an overriding public interest that would justify information sharing and wherever possible involve the appropriate Caldicott Guardian.

➢ Decisions about who needs to know and what needs to be known should be taken on a case by case basis, within agency policies and the constraints of the legal framework.

➢ Principles of confidentiality designed to safeguard and promote the interests of an adult should not be confused with those designed to protect the management interests of an organisation.

➢ In certain circumstances, it will be necessary to exchange or disclose personal information.
Information Sharing Agreement

The National Health Service Act 2006 Section 75 Partnership Arrangements

New powers to enable health and local authority partners to work together more effectively came into force on 1st April 2000. These were outlined in Section 31 of the 1999 Health Act which introduced a duty on NHS bodies and local authorities to work in partnership with one another.

Section 31 has since been repealed and replaced, for England, by Section 75 of the National Health Service Act 2006 ("the NHS Act 2006"), which in turn has been amended by provisions in the Health and Social Care Act 2012. Section 75 of NHS Act 2006 deals with partnership arrangements between NHS bodies and local authorities and enables NHS bodies and local authorities to enter into arrangements for pooling resources and delegating certain NHS and local authority health related functions to the other partner/s, provided that would lead to an improvement in the way those functions are exercised. Regulation 9(3)(h) of the NHS Bodies and Local Authorities Partnership Arrangements Regulations 2000 provides that where partners enter arrangements for the exercise by local authorities of NHS functions together with the exercise of their own health related functions, the agreement must be in writing and must specify the arrangements in place for sharing of information between NHS bodies and local authorities.

The Data Protection Act 1998

Anyone processing personal data must comply with the eight enforceable principles governing the use of personal information. They say that data must be:

1) Fair and lawful

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. Also the processing must adhere to the Fair Processing Code as published by the Information Commissioner’s Office.

2) Use for specified purposes

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

3) Adequate, relevant and not excessive

Personal data shall be adequate, relevant and not excessive in relation to the purpose.

4) Accurate and up to date

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

5) Do not keep longer than necessary
Information Sharing Agreement

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

6) Rights given under the act

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

7) Unauthorised or unlawful processing, loss, destruction and damage

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) Disclosure outside Europe

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.

Information covers both facts and opinions about the individual. It also includes information regarding the intentions of the data controller towards the individual, although in some limited circumstances exemptions will apply. With 'Processing,' the definition is far wider than before. For example, it incorporates the concepts of 'obtaining,' holding' and 'disclosing'.

9) Schedule 2 — Conditions relevant for the purposes of the first principle:

Processing of any Personal Data

Schedule 2 specifies the conditions relevant for the fair and lawful processing of personal data. Personal data is information which relates to a living individual who can be identified from that data, or from that data and other information which is, or is likely to come into, the possession of the data controller. This includes opinions about the individual and any indications of the organisation’s intentions in respect of that individual.

The conditions are:

- The data subject has given consent, or the processing is necessary for:
- The performance of a contract of which the data subject is a party
- The compliance of a legal obligation to which the data controller is subject
- The protection of the vital interests of the data subject
- Administering justice, or for exercising statutory, governmental, or other public functions
Information Sharing Agreement

➢ The legitimate interests of the Data Controller

In practice this means Data Controllers must
➢ have legitimate grounds for collecting and using the personal data
➢ not use data in ways that have unjustified adverse effects on the individual concerned
➢ be transparent about how they intend to use the data, and give individuals appropriate privacy notices when collecting their personal data
➢ handle people’s personal data only in ways they would reasonably expect; and
➢ make sure they do not do anything unlawful with the data.

10) Schedule 3 – Conditions relevant for the first principle: Processing of Sensitive Personal Data

Sensitive data is ‘personal data’ that contains information as to an individual’s racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical/mental health, sexual life, or criminal offending.

The conditions are:

The data subject has given explicit consent, or the processing:
➢ Is necessary to comply with employment law
➢ Is necessary for the purpose of, or in connection with legal proceedings
➢ Is necessary for the protection of the vital interests (a) of the individual (where their consent cannot be obtained), or (b) another person
➢ The information has deliberately been made public by the data subject
➢ Is carried out by a not for profit organisation and does not include disclosure to a third party
➢ Is necessary in relation to legal proceedings
➢ Is necessary for the administration of justice or for exercising statutory of governmental functions
➢ Is necessary for medical purposes and undertaken by someone subject to an equivalent duty of confidentiality
➢ Is necessary for monitoring equality of opportunity

Human Rights Act 1998 and Article 8 of the ECHR

The Human Rights Act 1998 contains provisions which have the effect of codifying the protections set out in the European Convention of Human Rights ("the ECHR")
Information Sharing Agreement

into UK law. Of special relevance to the sharing of personal information, is Article 8 of the ECHR which provides that:

Everyone has the right to respect for his private and family life, his home and his correspondence.
There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Article 8 means that people, in ordinary circumstances, have the right to withhold personal information if they choose and, in conjunction, with the common law right of confidentiality, to decline to allow personal information to be shared.

The Common Law Duty of Confidentiality

The common law duty of confidentiality is derived from case law rather than statute and requires that unless there is a statutory requirement to use information that has been provided in confidence, it should only be used for purposes that the subject has been informed about and consented to. In certain circumstances, this also applies to the deceased. The duty is not absolute but should only be overridden if the holder of the information can justify disclosure as being in the public interest, for example, to protect others from harm.

Caldicott Principles

The Caldicott Committee was set up in 1996 by the Chief Medical Officer to review “all patient-identifiable information which passes from 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”.

The Committee published six principles, or standards, that are now accepted as the foundation of good practice for handling personal identifiable information:

Principle 1- Justify the purpose (s)
Every proposed use or transfer of personally-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appropriate Guardian.

Principle 2- Do not use personally-identifiable information unless it is absolutely necessary
Personally identifiable information items should not be used unless there is no alternative.
Information Sharing Agreement

Principle 3- Use the minimum necessary personally-identifiable information
Where use of personally identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identifiably.

Principle 4- Access to information should be on a strict need to know basis
Only those individuals who need access to person identifiable information should have access to it, in order to undertake tasks within their job role, or tasks which they have expressly been given responsibility for.

Principle 5 – Everyone with access to it should be aware of their responsibilities
Action should be taken to ensure that staff handling person identifiable information are aware of their responsibilities and obligations to respect an individual’s confidentiality.

Principle 6 – Understand and comply with the law
Every use of person identifiable information should be lawful.

Caldicott Review 2013

The implications of the Caldicott review for safeguarding adults are:

- Information may only be shared on a 'need to know' basis when it is in the interests of the adult
- Confidentiality must not be confused with secrecy
- Informed consent should be obtained but, if this is not possible and other adults are at risk of abuse or neglect, it may be necessary to override the requirement and
- It is inappropriate for agencies to give assurances of absolute confidentiality in cases where there are concerns about abuse, particularly in those situations when other adults may be at risk.

Computer Misuse Act 1990

This Act makes it a criminal offence to access any part of a computer system, programs and/or data that a user is not entitled to access. Each organisation will adhere to the requirements of the Computer Misuse Act 1990 by ensuring staff are made aware of their responsibilities regarding the misuse of computers for personal gain or other fraudulent activities. Any member of staff found to have contravened this Act would be considered to have committed a disciplinary offence and be dealt with accordingly.
Information Sharing Agreement

The NHS Confidentiality Code of Practice

The Confidentiality Code of Practice is to ensure that information given by the patient is treated as confidential information and only to be divulged on a need to know basis. All staff are obliged to adhere to this procedure.

The Mental Health Act 1983

The 1983 Act is largely concerned with the circumstances in which a person with a mental disorder can be detained for treatment for that disorder without his or her consent. It also sets out the processes that must be followed and the safeguards for patients, to ensure that they are not inappropriately detained or treated without their consent. The main purpose of the legislation is to ensure that people with serious mental disorders which threaten their health or safety or the safety of the public can be treated irrespective of their consent where it is necessary to prevent them from harming themselves or others.

Mental Capacity Act 2005

From 1 October 2007 this Act is fully in force in England and Wales. It impacts on all staff working with or caring for adults (16+) who lack mental capacity (or have impaired capacity) to make their own decisions about health, social care and financial matters.

The Act makes clear who has authority to make decisions in certain situations and sets out statutory principles which must guide decision-making.

Doctors have a legal duty to have regard to the Code of Practice in their day to day decisions about the treatment and care of incapacitated patients. So it is important that doctors take steps to familiarise themselves with the legal principles, and the provisions of the Code which are of most relevance to their areas of practice.

Social Care Record Guarantee

"Your local authority has a range of duties to support and care for those most in need in the community. To do this we provide a range of services, such as:

- assessing your, or your and your carer's, needs;
- providing care in your home;
- taking steps to protect you if you are at risk of harm;
- paying someone to help care for you;
- supporting you in a residential home; and
- providing a foster carer (if you need one).

To do this, we must hold records about you, your personal circumstances and the care you are receiving or may need to receive in the future.

V1; Aug 2015
Information Sharing Agreement

This guarantee is our commitment that we will use records about you in ways that respect your rights and promote your health and wellbeing.

'Personal information' and 'Sensitive Personal Information'

Personal Information

'Personal information' is information that can be used, directly or indirectly, to identify an individual person.

The Data Protection Act 1998 defines personal data as relating to 'a living individual who can be identified':

from those data, or
from those data and other information which is in the possession of, or likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual [DPA 1 (1)].

Information that directly names or identifies the individual is covered; but so also is information that could be used with other information to identify the person. Relevant to this Information Sharing Agreement are such situations in which, for example, a professional might use his or her experience of working with a patient or client as an unidentified 'case study' for team training, in such a way as would allow other professionals to know who was being referred to because they too had knowledge of the case.

For the purposes of this Agreement, which covers providing health and social care services to adults, all individual patient or client information should, ordinarily, be considered as at least 'personal information'.

Sensitive Personal Information

The Data Protection Act also determines that beyond 'personal information', there is 'sensitive personal information.' Sensitive personal data, in the Act, means personal data that relates to:

Racial/ethnic origin of the data subject;
Political opinions;
Religious or similar beliefs;
Membership of a trade union;
Physical or mental health or condition;
Sexual life; and

The commission or alleged commission by him/her of an offence and any related proceedings.

The Data Protection Act provides individuals with certain rights with regard to personal and sensitive personal information, and also places certain
Information Sharing Agreement

responsibilities on professionals in the processing of personal and sensitive personal information. These are discussed below.

‘Ownership’ of personal information

Where two agencies share information the agency that discloses the information retains legal ‘ownership’ of that information. This means that:

The source of the shared information must be identified and recorded as the ‘data owner’

The purpose for which that information was shared must be recorded

Any subsequent intention to share information beyond the original purpose, known as ‘secondary disclosure’, is referred to the data owner

Secondary disclosure must not occur without the agreement of the data owner, unless there is a legal power and necessity to do so

However, ultimately, data subjects are the owners of their data and have a right to influence how their data is used (even if needs must override this in some circumstances).
16. **Appendix 2 – List of ISAB Partner Organisations party to this agreement**

<table>
<thead>
<tr>
<th>Organisation</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Islington Council</td>
<td>7 Newington Barrow Way, London, N7 7EP</td>
</tr>
<tr>
<td>Islington Clinical Commissioning Group</td>
<td>338-346 Goswell Road, London, EC1V 7LQ</td>
</tr>
<tr>
<td>Whittington Health NHS Trust</td>
<td>The Whittington Hospital, Magdala Avenue, N19 5NF</td>
</tr>
<tr>
<td>Camden and Islington Mental Health NHS Foundation Trust</td>
<td>4th Floor, East Wing, St Pancras Hospital, 4 St Pancras Way, London, NW1 0PE</td>
</tr>
<tr>
<td>London Metropolitan Police</td>
<td>Islington Police Station, 2 Tolpuddle Street, N1 0YY</td>
</tr>
<tr>
<td>Moorfields Eye Hospital NHS Foundation Trust</td>
<td>162 City Rd, London, EC1V 2PD</td>
</tr>
<tr>
<td>London Fire Brigade</td>
<td>Holloway, 262-268 Hornsey Road, N7 7QT</td>
</tr>
<tr>
<td>London Ambulance Trust</td>
<td>Islington, 278 Upper Street, N1 2TZ</td>
</tr>
<tr>
<td>Address</td>
<td>Contact Information</td>
</tr>
<tr>
<td>---------</td>
<td>---------------------</td>
</tr>
<tr>
<td>220 Waterloo Rd</td>
<td>London SE1 8SD</td>
</tr>
<tr>
<td>Healthwatch</td>
<td>200 Pentonville Road London N1 9JP</td>
</tr>
<tr>
<td>London Probation Service</td>
<td>151 Buckingham Palace Road 1st Floor London SW1W 9SZ</td>
</tr>
<tr>
<td>Community Rehabilitation Company</td>
<td>151 Buckingham Palace Road 1st Floor London SW1W 9SZ</td>
</tr>
<tr>
<td>Single Homeless Project</td>
<td>245 Gray's Inn Road London WC1X 8QY</td>
</tr>
<tr>
<td>Age UK</td>
<td>6-9 Manor Gardens London N7 6LA</td>
</tr>
<tr>
<td>Notting Hill Housing Group</td>
<td>Bruce Kendrick House, 2 Killick Street London N1 9FL</td>
</tr>
</tbody>
</table>
17. **Appendix 3 – sensitive data sets**

Sensitive personal data is defined in the Data Protection Act 1998 as personal data consisting of information as to:

- a person’s physical/mental health
- criminal proceedings in respect of
- person
- the commission or alleged commission of a criminal offence by a person
- a person’s racial or ethnic origin
- their sexual life
- whether a person is a member of a trade union
- their political opinions
- their religious beliefs or belief of a similar nature
- Whilst not defined as sensitive personal data in the Data Protection Act, other information considered to be sensitive, requiring appropriate management, is:
  - protected whereabouts
  - National Insurance numbers
  - bank account details
  - identification credentials