Haringey Safeguarding Adults

Multi Agency Information Sharing Protocol and Agreement 2016

Status: Draft

Version: 0.3

Reviewed: September 2016

Foreword:

The Care Act 2014 establishes criteria which require the sharing of confidential information. It is important, therefore, to establish, within the context of Safeguarding Adults, a Protocol and Agreement for sharing information between the partner agencies that have committed to the Multi-Agency Agreement in the Safeguarding Adults Procedures.

This Agreement covers the sharing of information for any of the purposes listed below and comprises the common principles and procedures, which will be adopted wherever, and whenever these agencies have to share information for these purposes.

The effective and timely sharing of information is essential to deliver high quality services focussed on the needs of the individual. In Haringey, we encourage a culture where information is shared with confidence as part of routine service delivery. Sharing information is vital to prevent and detect crime and to ensure that our residents are protected from suffering harm from abuse or neglect.

This Information Sharing Protocol (ISP) explains the terms under which partner organisations have agreed to share information and the practical steps that need to be taken to ensure compliance with those terms. Partner Organisations are fully committed to share information and have agreed to comply with the procedures as set out in this protocol.

The absence of a protocol should not prevent sharing information.

If you need to share information outside of the terms of this protocol or with agencies that are not party to this protocol you should follow the guidance as outlined in Haringey's *Simple Guide to Sharing Information (see appendix E)*.

The guiding rule is: if you need to share information in order to protect someone from harm or criminal activity, you must do so.

An information sharing guide for practitioners working with vulnerable adults accompanies this protocol. The guide should be given to all relevant staff.

Contents Page

Document Control

Issue	Date	Author	Comments	Approval
0.1	January 2015	Helen Constantine	Introduction of Care Act 2014	
0.2	April 2016	Helen Constantine	Comments from SAB QA subgroup	
0.3	September 2016	Helen Constantine	Comments from SAB partner agencies	

This protocol became effective on add date/15 November 2016

This protocol will be reviewed annually and subject to change dependent on any changes legislative changes and national guidance - please refer to Section 10 of this document (Review and Audit).

Any significant amendments to this protocol made before the review date stated above will need to be approved in principle by all Partner Organisations and will only be effective until the review date. All significant amendments will need to be endorsed by the Partner Organisations at the review date

1. Purpose

1.1 This Information Sharing Protocol (ISP) is intended to meet the recommendation in paragraph 15.157 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.

1.2 This ISP is an agreement between Partner Organisations (see appendix A for a list of parties to this protocol) specifically to facilitate and govern information sharing. Its purpose is:

- To facilitate the secure exchange of information, where necessary to ensure the safeguarding of Adults in Haringey.
- To provide a framework for the secure and confidential sharing of personal information between the partner organisations.

1.3 For the purposes of this protocol, an individual may be referred to as a patient, client or data subject.

1.4 ISPs are not required before front-line practitioners can share information about an individual. By itself, the lack of an ISP must never be a reason for not sharing information that could help a practitioner deliver services to an individual.

2. Background

2.1 The sharing of personal information between organisations is vital to ensure co-ordinated and seamless provision of services that are protective and supportive.

Sharing information will:

- Provide professionals with background information on a named person;
- Reduce the need for information to be repeated to different professionals;
- Enable professionals to keep track of their interventions and the status of their contact with the named person;
- Ensure that the named person can be traced;
- Identify individuals who have not benefited from service support in the past;
- Reduce duplication of data collection across partner agencies;
- Improve the consistency and accuracy of management information; and
- Progress assessment and care planning on a multi-agency/professional basis.

2.2 Appropriate information sharing amongst partner organisations of the Haringey Safeguarding Adults Board (HSAB) is essential to safeguard and promote the wellbeing of adults at risk in Haringey.

2.3 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.

2.4 HSAB 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.

2.5 It is the expectation that staff and volunteers in HSAB 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;
- if consent is refused or no response is received, decide whether disclosure should be made in the absence of consent;
- assist the HSAB to meet its objectives as defined in its Constitution ; and
- to enable all HSAB partners to work together effectively in line with relevant legislation, including The Data Protection Act 1998, The Children Act 1989 and 2004, Human Rights Act 1998, the Care Act 2014 and the Mental Capacity Act 2005.

2.6 Practitioners working in adults' services are aware that problems faced by clients who have parenting responsibilities, are often likely to affect children and other family members, for example: vermin, alcohol and drugs or where there is a dangerous weapon in the house. However this information is not always shared and opportunities to put preventative support in place for the children and family are missed. Where an adult receiving services is a parent or carer, sharing information where appropriate with colleagues in children's services could ensure that any additional support required for their children can be provided early.

2.7 The MASH is a multi-agency safeguarding hub, which brings together a variety of agencies into an integrated multi-agency team, where they can share intelligence on vulnerable children, families and adults. Haringey's MASH will build on the existing First Response Multi Agency Team (FRMAT) which has been operating since May 2010. It co-locates Metropolitan Police, Health colleagues and Social Workers, together with support from education and housing. MASH will enhance this service through the additional police intelligence, and the co-location of other agencies such as Adult Safeguarding, Probation and Mental Health.

2.8 The key objectives of MASH are to:

- Identify risks to children and adults at the earliest possible point;
- Ensure better information sharing and therefore more effective interventions;
- Deliver cashable efficiencies in the longer term; and
- Identify and reduce harm, crime and anti social behaviour.

2.9 The Safeguarding Adult Service contributes to the multi-agency approach to protect children and young people at both a strategic and operational level. Strategic links are strengthened by reciprocal membership of the Safeguarding Adults Board and the Local Safeguarding Children's Board, by the second tier management who hold the overall responsibility and leadership of safeguarding in their respective areas. The Safeguarding Adults Plan for 2012/13 highlights the continued commitment to ensuring safe, quality arrangements to safeguard children and young people.

There is commitment to joint decision making at the Multi Agency Risk Assessment Conference (MARAC) and Multi Agency Public Protection Arrangements (MAPPA).

2.10 In March 2012 the Home Office published a cross-departmental plan to tackle hate crime setting out the strategic direction the Government wishes to take to address this issue, looking in particular at:

- The different types of hate crime highlighted by the plan;
- The key objectives of the plan and their relevance for local authorities;
- The wider policy context; and
- The reaction from organisations in the sector.

The Home Office has set a national direction to combat hate crime and is made up of three key areas, including:

- Improving the Response to Hate Crime: criminal justice system more effective and offenders are dealt with more robustly. *Councils and other local partners*

work jointly with the criminal justice system to bring offenders to justice – making available information on hate crime and local support services.

Sharing information is vital to prevent and detect crime and to ensure that our residents are protected from suffering harm from abuse or neglect. Haringey's Crime and Disorder Information Sharing Protocol explains the terms under which partner organisations have agreed to share information and the practical steps that need to be taken to ensure compliance with those terms. The Protocol, a practitioners' guide to sharing information, the request/disclosure and consent forms can be accessed via the following link: http://contentmanager/index/community_and_leisure/communitysafety/crime_and_disorder_-_information_sharing_protocol.htm?debugstate=3.

To sign up to the Crime and Disorder Information Sharing Protocol, please contact Eliza Meechan (eliza.meechan@haringey.gov.uk). A senior member of your organisation will need to confirm in writing that they commit to the terms of the Information Sharing Protocol and a Designated Liaison Officer will need to be identified.

2.11 The London Ambulance Service (LAS) works to 32 local authorities' pan-London procedure. Each ambulance station complex has a nominated Safeguarding Lead, usually the ambulance operations manager or a delegated local manager, who has responsibility to represent LAS at serious case reviews and strategy meetings. LAS' patient experiences department act as the clearing house and *initial contact* should always be made via their Safeguarding email address - safeguarding.las@nhs.net.

.

3 Types of information

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.

3.1 Personal information

3.1.1 The Data Protection Act 1998 defines 'personal information' as information relating to a living individual who can be identified either from that information or from that information in conjunction with other information that is in, or is likely to come into, the possession of the data controller.

3.1.2 Information being shared includes:

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

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

3.1.3 The definition of personal information is technology neutral; the definition is not influenced by how the information is stored (e.g. on a computer database, paper filing system, microfiche, portable memory stick).

3.1.1 Where it is necessary for information to be shared, personal information will be shared only on a need-to-know basis and only covers interagency sharing of information for purposes of safeguarding adults. Appendix A summarises how

information can be shared within the terms of Haringey Safeguarding Adult's Multi-Agency Information Sharing Protocol.

3.1.2 Any duty of confidentiality will be respected unless there is an overriding 'public interest' to disclose the information and if there is a 'legitimate purpose' to sharing (see section 5). Where the disclosure would breach client confidentiality the request should be referred to a designated manager - unless exceptional circumstances apply, e.g. where there is a need for urgent medical treatment. Managers should have access to a source of advice and support on information sharing issues. This may be a Caldicott Guardian. In the absence of advice from their own agency officers and/or managers should contact: Designated Safeguarding Adults Lead on 0208 489 3106.

3.1.3 The reasons for breaching client confidentiality must be fully recorded and clearly referenced to the evidence and information on which the decision is based. This must include details of any third parties and details of all the information/evidence they have been given.

3.2 Depersonalised information

3.2.1 Depersonalised information encompasses any information that does not and cannot be used to establish the identity of a living person, having had all identifiers removed.

3.2.2 Partner Organisations accept that there are no legal restrictions on the exchange of depersonalised information, although a duty of confidence may apply in certain circumstances, or a copyright, contractual or other legal restriction may prevent the information being disclosed to Partner Organisations.

3.2.3 Information shared between Partner Organisations should be limited for the purposes of the enquiry. If the purpose of this protocol can be achieved using depersonalised information, then this should be the preferred method used by officers. For example, in assessing crime hotspots geographic information that does not identify living individuals might be used for strategic planning purposes.

3.2.4 Partner Organisations recognise that great care must be taken when depersonalising information and that the Information Commissioner has stated that even a post-code or address can reveal the identity of an individual. Partner Organisations are also aware that it may be possible for an individual's identity to be revealed by comparing several sets of depersonalised data.

3.3 Non-personal information

3.3.1 Partner Organisations understand that non-personal information is information that does not, nor has ever, referred to individuals.

4 Consent

4.1 Many issues surrounding the disclosure of personal information can be avoided if the consent of the individual has been sought and obtained. Obtaining consent remains a matter of good practice and in circumstances where it is appropriate and possible, informed consent should be sought. (There is a 'Consent Form' at appendix C of this protocol that can be used if signed consent has not already been obtained as part of the assessment or referral process).

4.2 Practitioners should encourage clients to see information sharing (and giving their consent to share their personal information) in a positive light, as something which makes it easier for them to receive the services that they need.

4.3 Whose consent to seek:

4.3.1 All people deemed to be Gillick competent are presumed, in law, to have the capacity to give or withhold their consent to sharing of confidential information, unless there is evidence to the contrary. If an adult lacks the capacity to take their own decisions, then professionals should share information that is in their 'best interests'. A 'best interests' checklist is set out in section 4 of The Mental Capacity Act 2005 http://www.opsi.gov.uk/acts/acts2005/ukpga_20050009_en_1. The Act provides a statutory framework to empower and protect vulnerable people who may not be able to make their own decisions. It makes it clear who can take decisions in which situations and how they should go about this. The *Act* defines the term 'a person who lacks capacity' as a person who lacks capacity to make a particular decision or take a particular action for themselves, at the time the decision or action needs to be taken.

4.3.2 In recent years, the subject of undue influence has received increasing attention in the field of elder abuse prevention. Simply stated, undue influence is when an individual who is stronger or more powerful gets a weaker individual to do something that the weaker person would not have done otherwise. For example, the stronger may isolate the weaker person, promote dependency, or induce fear and distrust of others. Because undue influence (like mental capacity) raises the question of whether an individual is acting freely, the two concepts are often confused. Although diminished mental capacity may contribute to a person's vulnerability to undue influence, the two are distinct and cognitive assessments cannot identify the presence of undue influence. It is typically courts that make determinations of whether or not undue influence has been exercised. In doing so, they consider a variety of factors, including whether the transaction took place at an appropriate time and in an appropriate setting and whether the older person was pressured into acting quickly or discouraged from seeking advice from others. Courts also consider the relationship between the parties, and the "fairness" of the transaction.

5. Sharing information without consent

5.1 Practitioners should not seek consent when they are required by law to share information through a statutory duty or by a court order. Consent should also not be sought if doing so would:

- place a person (the individual, family member, staff or a third party) at increased risk of significant harm if a child, or serious harm if an adult; or
- prejudice the prevention, detection or prosecution of a serious crime; or
- lead to an unjustified delay in making enquiries about allegations of significant harm to a child, or serious harm to an adult.

5.2 An example of where not sharing information could place a person at increased risk of significant harm is in a situation where a vulnerable member of the public requires urgent medical assistance and information is not shared between partner agencies. In emergency medical situations information should always be shared between partner agencies. In circumstances where vulnerable members of the public carry emergency alert cards, the instructions on the card should be followed in line with service procedures.

5.3 If consent has not been sought, or sought and withheld, the agency must consider if there is a 'legitimate purpose' for sharing the information and if it is in the 'public interest' to share; and clearly record the reasons for doing so.

5.4 The reasons underlying any decision to disclose or not to disclose information under this protocol should be carefully recorded, and communicated to those who have been consulted prior to the disclosure. Recipients should be reminded that the information is confidential and should be informed of the reasons for disclosure to themselves. Decisions to refuse disclosure requests should be explained. **Consent lasts as long as co-ordinated inter-agency services are required, unless it is withdrawn. Individuals have the right to withdraw consent after they have given it and organisations to record accordingly.**

5.5 Legitimate Purpose

5.5.1 Partner Organisations understand the 'Legitimate Purpose' criteria to include:

- Preventing serious harm to an adult - including through prevention, detection and prosecution of a serious crime.
- Providing urgent medical treatment to an adult.

5.6 Public Interest

5.6.1 Partner Organisations understand the 'Public Interest' criteria to include:

- When there is evidence or reasonable cause to believe that an adult is suffering, or it at risk of suffering, serious harm;
- To prevent the adult from harming someone else;
- The promotion of welfare of the adult;
- Detecting crime;
- Apprehending Offenders;
- Maintaining public safety; and
- Administration of justice.

5.6.2 When considering whether disclosure is in the public interest, 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 by partner organisation(s) and documented.

6 Requesting Information under this protocol

6.1 Where staff have reasonable cause to believe that an adult may be at risk of suffering serious harm, they should always consider referring their concerns to social services or to the local police force – in line with the Haringey Safeguarding Adults Board (HSAB) Policies and Procedures. In some situations staff may be unsure whether 'a concern' that an adult may be at risk of suffering serious harm, constitutes 'a reasonable cause to believe'. In these situations, the concern must not be ignored. When in doubt, staff should always talk to a lead person on safeguarding to help them decide what to do – for example: their manager or an experienced and trusted colleague. If those officers are in doubt, then they should speak to a Caldicott Guardian. Staff should try to protect the identity of the individual (wherever possible), until they have established a reasonable cause for their belief. Where staff need information from a Partner Organisation party to this protocol they should submit their inquiry in writing using the 'Request/Disclosure' form found in appendix C of this protocol.

6.2 Where appropriate, the requesting officer must also supply the Partner Organisation with evidence of the client's consent. (For more information on 'Consent' see section 4). The 'Request/Disclosure' form must be added to the client's record.

6.3 The requesting and disclosing officers will ensure that any personal information is transferred in secure manner (for more information on 'Security' see section 8.5)

6.4 Routine exchanges of information, such as asking whether a person is known to a service, should be requested formally (and agreed by the supplying partner) on one form. There is no need to submit a separate form for each occurrence. Such procedure is subject to a continued review by participating Partner Organisations and by a further formal request form every 9 months if de-personalised or non-personal or 6 months if personal.

7 Disclosing Information under this protocol

7.1 Staff disclosing information must always consider the safety and welfare of the client when making decisions on whether to share information about them. For example, where there is concern that an adult may be suffering or is at risk of suffering serious harm, and then the adult's safety and welfare must be the overriding consideration.

7.2 Officers disclosing information must ensure that the requesting officer has supplied a completed 'Request/Disclosure' form and, where appropriate, evidence of the client's consent (for more details on 'Consent' see section 4).

7.3 The disclosing officer must also ensure that any information disclosed is:

- necessary for the purpose for which they are sharing it;
- accurate and up-to-date;
- depersonalised (where appropriate);
- shared only with those people who need to see it; and
- transferred securely.

7.4 The disclosing officer must complete the appropriate section of the 'Request/Disclosure' Form and save it in line with service procedures.

8 Data Protection

8.1 Data Protection Act

8.1.1 Partner Organisations agree to comply at all times with data protection legislation and other legal requirements relating to confidentiality.

8.2 Fair Processing

8.2.1 The Data Protection Act 1998 requires that when personal information is collected from a data subject, they are told what it will be used for and who the information will be shared with.

8.2.2. When collecting information from clients, staff in partner organisations should explain:

- What is done with the information;
- The reason why professionals are capturing it; *and*
- Who the information can be routinely shared with.

8.2.3 Partner Organisations will ensure that their 'Fair Processing Notices' are kept up-to-date and provide an accurate explanation of the information sharing activities that are being undertaken.

8.3 Retention Periods

8.3.1 All partner organisations who are party to this protocol will put in place policies and procedures governing the retention and destruction of records containing personal information retained within their systems.

8.3.2 As a general rule, partner organisations agree that personal information that has been shared will be destroyed once it no longer is of relevance to the initial inquiry.

8.4 Data Quality

8.4.1 Partner organisations will notify the source of the information if they discover that the information is inaccurate or inadequate for the purpose. The source will be responsible for correcting the data and notifying all other recipients in writing.

8.5 Security

8.5.1 Personal information will be kept securely within a computer system or otherwise physically secure with appropriate levels of staff access in line with party organisations' information security policies and procedures. These policies and procedures should be based on national standards and guidance.

8.5.2 Staff in Partner Organisations involved in information sharing under this protocol must:

- Be fully aware of their responsibilities under the protocol mentioned above, together with the Data Protection Act and Duty of Confidentiality.

- Use information only for the purpose stated in the original request for information.
- First obtain consent from the disclosing organisation, if they wish to pass the information onto a third party. (In a high risk situation involving safeguarding, this may not always be a reasonable requirement. In emergencies, the public interest disclosure is a sufficient exemption to override this requirement).
- Store hard copies of the request/disclosure and consent forms in a lockable container when not in use, and a clear desk policy implemented.

8.5.3 If the information is held electronically, access must be restricted only to persons with a genuine 'need to know' the information.

8.5.4 Once this information is no longer required, it must be destroyed. Only the minimum amount of personal information should be retained in line with the records retention rates as per organisational / NHS Guidance which is necessary to achieve the purpose for which it was obtained.

8.5.5 There is purpose specific information sharing arrangements for Haringey Multi Agency Safeguarding Hub. Any e-mail communication will be by way of secure, appropriate and approved methods. The sharing of any information must be done via secure email, meaning only email addresses with .pnn, .gcsx, .cjsm, .gsi and nhs.net will be used anything other than this should be recorded initially and followed up as an internal breach or incident.

8.5.6 Each Partner Organisation is responsible for ensuring that the appropriate staff (including interim or agency staff) are adequately trained in respect of all matters covered by this protocol. All temporary and agency staff will be appropriately briefed on their responsibilities as part of their induction.

8.6 Subject Access Requests

8.6.1 The Data Protection Act gives people the right to apply to an organisation that holds personal information about them for access to that information. The exercise of this right is referred to as a subject access request. People may exercise this right on their own behalf or through a representative. Where people do not have the mental capacity to make a request on their own behalf, because they are too young or for some other reason, their parent or person with Power of Attorney may make the request on their behalf. All partner organisations that are party to this protocol will put in place procedures for handling requests for personal information.

8.6.2 The right of subject access applies to all personal information held by an organisation about that data subject regardless of whether or not that organisation is the "owner" or "source" of the information. The information must be disclosed to the data subject unless one of the exemptions in the Data Protection Act applies. It may be appropriate for the organisation that has

received the subject access request to consult with the source of the information they hold to discuss whether the information is subject to an exemption.

9 Freedom of Information

9.1 The Freedom of Information Act 2000 (FOI) enables any member of the public to apply for access to information held by bodies across the public sector. The Act provides a general right of access to information held by public authorities in the course of carrying out their public functions, subject to some exemptions. This right does not extend to personal information, which is largely exempt from the Freedom of Information Act.

9.2 Partner Organisations will ensure that this protocol is included in their Publication Scheme.

10 Review and Audit

10.1 The protocol will be reviewed by the Partner Organisations every three years unless there is a requirement due to national legislation.

10.2 The review is to be undertaken jointly by officers agreed by the Partner Organisations unless agreed by the Partner Organisations for a single Partner Organisation to undertake the review. This work will be coordinated by the HSAB. At each review date the respective board will pull together a review group made up of parties to the protocol, and identify operational problems, new legislation and highlight any proposed amendments to be agreed.

10.3 Partner Organisations may audit compliance with this protocol.

10.4 Partner Organisations agree to assist other Partner Organisations during the audit process as long as reasonable notice is given in writing detailing the scope of the audit process and they do not object.

11 Key Legislation

11.1 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 or to 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. When considering whether disclosure is in the public interest, 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 by partner organisation(s) and documented.

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.

11.2 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 partners/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.

11.3 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:** 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. Personal data 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:

2. The data subject has given consent, or the processing is necessary for:

3. The performance of a contract of which the data subject is a party

4. The compliance of a legal obligation to which the data controller is subject

5. The protection of the vital interests of the data subject

6. Administering justice, or for exercising statutory, governmental, or other public functions

7. 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 is 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

11.4 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") 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.

11.5 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.

11.6 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 seven 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.

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.

Principle 7 - 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.

11.7 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.

11.8 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.

11.9 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.

11.10 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.

11.11Mental 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.

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

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

11.14 '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).

11.15 Pan London Multi-Agency Adult Safeguarding Adults Policy & Procedures

This protocol and agreement supplements the London Multi-Agency Adult Safeguarding Policy & Procedures and reflects the local practice guidance for the sharing of information in relation to safeguarding.

The Care Act 2014 Section 45 'supply of information' duty covers the responsibilities of others to comply with requests for information.

List of Appendices

A. Parties to the protocol

B. Glossary of terms

C. Consent form

D. Additional legislation relating to this protocol

E. Simple guide to information sharing

F. Caldicott principles

G. Procedure document for NHS Haringey Clinical Commissioning Group and ACS use of Mosaic for the Single Assessment Process, and associated common activity

Appendix A: Parties to the protocol

Organisation	Representative
Haringey Council	**Beverley Tarka** Director of Adult Social Services and Caldicott Guardian
Homes for Haringey	**Andrew Billany** Managing Director
NHS Haringey Clinical Commissioning Group	**Dr Peter Christian** Chair, Clinical Commissioning Group
North Middlesex University Hospital	**Elizabeth McManus** Chief Executive
Whittington Health	**Simon Pleydell** Chief Executive
Barnet, Enfield and Haringey Mental Health NHS Trust	**Mary Sexton** Executive Director of Nursing, Quality and Governance
Metropolitan Police Service (Haringey Division)	**Helen Millichap** Borough Commander
London Fire Brigade	**Simon Amos** Borough Commander Haringey
Bridge Renewal Trust	**Geoffrey Ocen** Chief Executive Officer

Appendix B: Glossary

Caldicott Guardian is a person with responsibility for policies that safeguard the confidentiality of patient information.

Confidential is information that has a degree of sensitivity and value and is subject to a duty of confidence.

Consent is when someone accepts or agrees to something that somebody else proposes. For consent to be legal and proper, the person consenting needs to have sufficient mental capacity to understand the implications and ramifications of his or her actions.

Information Sharing Protocol (ISP) - is a signed agreement between two or more partner organisations relating to a specified information sharing activity. An ISP explains the terms under which the organisations have agreed to share information and the practical steps that need to be taken to ensure compliance with those terms.

Practitioner is the generic term used in this guidance to cover everyone who works with adults and children and young people.

Public interest is the interests of the community as a whole, or a group within the community or individuals.

Serious harm for the purposes of this guidance can be either physical or mental trauma to an adult.

Significant harm – there are no absolute criteria on which to rely when judging what constitutes significant harm. Consideration of the severity of ill treatment may include the degree and the extent of physical harm, the duration and frequency of abuse and neglect, the extent of premeditation, and the presence or degree of threat, coercion, sadism, and bizarre or unusual elements.

Well-being has a legal definition based on the five *Every Child Matters* outcomes; the achievement of these outcomes is in part dependent upon the effective work to safeguard and promote the welfare of children, young people and families.

Appendix C: Safeguarding Adults Multi-Agency Information Sharing Protocol Request/Disclosure Form

Requesting Officer's Ref:	
Disclosing Officer's Ref:	

PART INFORMATION REQUESTED - (to be completed by requesting officer)

Information requested by:

Name:	
Job Role:	
Organisation/Department:	
Contact phone number:	
Email address:	

Information requested:

Describe the information required and the circumstance that have led to this request being made, including any names, addresses and dates of birth.				
Name:				
Address:				
DOB(ddmmyyyy):				
NHS Number				

Date information is required by (ddmmyyyy):			
If urgent, please state reason:			

Have you obtained consent to share information? (Please ensure that you attached the standardised 'Consent Form').	

If consent has not been obtained from the individual, please indicate for what purpose you require this information? (Please tick the relevant boxes as appropriate)

Preventing serious harm to an adult – *including through prevention, detection and prosecution of a serious crime.*	☐	Providing urgent medical treatment to an adult	☐	Implementing the Department of Health's 'No Secrets' agenda – *which aims to protect vulnerable adults from abuse.*	☐
In the 'public interest' and a 'legitimate purpose' to share *(for more information see section 5 of Haringey's Safeguarding Adults Multi-Disciplinary Information Sharing Protocol (ISP))*	☐	There is a statutory obligation or court order to share	☐	Please provide details:	

Signature of requesting officer:		Date:			

PART B - INFORMATION DISCLOSED – (to be completed by disclosing officer)

Disclosure Agreed:	Yes ☐ No ☐
Information attached to this form	Yes ☐ No ☐
Reason for declining request (if applicable):	

Information disclosed (Continue on a separate sheet if necessary, and remember to attach any additional sheets to this form)	

Information disclosed by:

Name:	
Department /Organisation:	
Contact phone number:	
Email address:	

Delivery method (please mark as appropriate): Email ☐ Fax ☐ Other (please specify)

Signature of disclosing officer: _____ Date supplied: _____

Haringey's Safeguarding Adults Multi-Agency Information Sharing Protocol - Consent Form

Requesting Officer's Ref:	
Disclosing Officer's Ref:	

Please provide the relevant information below:

Is this information about you? Yes ☐ No ☐ If 'No', who is the information about? Name: Address: DOB (ddmmyyyy) Are you are acting as: Parent/Guardian/Carer Other (please describe)

Have the reasons for requesting consent been explained to you?	Yes ☐ No ☐

I give:	
consent to disclose to:	

Information to which this consent applies:

Personal information and any relevant information, for the purposes of:

Your Name:				
Address:				
DOB (ddmmyyyy):				

Signature:				
Date (ddmmyyyy):				

Witnessed by requesting officer:

Name:				
Position:				
Signature:				
Date (ddmmyyyy):				

Appendix D: Additional legislation relating to this protocol

The principles and procedures embodied in this protocol are underpinned by the following legislation not outlined in the 'Key Legislation' section of this protocol:

- European Convention on Human Rights (given effect via the Human Rights Act 1998)
- Data Protection Act 1998
- Freedom of Information Act 2000
- Common Law Duty of Confidentiality
- Regulation of Investigatory Powers Act 2000
- Access to Health Records Act 1990
- Community Care (Delayed Discharges) Act 2003
- Health and Social Care Act 2012
- Health Act 2009
- The Children Act 2004
- The Local Government Act 2000
- The Education Act 1996
- The Education Act 2002
- The Learning and Skills Act 2000
- Children (Leaving Care) Act 2000
- Education (SEN) Regulations 2001
- NHS Bodies and Local Authorities Partnership Arrangements Regulations 2000
- The NHS (Venereal Diseases) Regulations 1974 and NHS Trusts (Venereal Diseases) Regulations 1991 The Abortion Regulations 1991
- The Human Fertilisation and Embryology Act 1990
- *Working Together to Safeguard Children* (HMG, 2006),
- Education and Inspections Act 2006
- Child Health Promotion Programme (DH, 2008)
- Local Government Act 1972 s224
- Local Government (Access to Information) Act 1985
- Human Rights Act 1998
- Public Records Act 1958 and 1967
- Regulation of Investigatory Powers Act 2000
- Mental Capacity Act 2005
- The Health Service (Control of Patient Information) Regulations 2002

Non-legislation includes;

- Caldicott Guidelines
- Local codes or standards relating to confidentiality
- Policies and Procedures around Haringey's Local Safeguarding Children's Board (LSCB) and Haringey's Safeguarding Adults Board (HSAB)

Appendix E: Simple Guide to information sharing

Information sharing with consent

If you have the person's consent, then it is ok to share personal information about them, providing they have the mental capacity to give consent. Obtaining explicit consent for information sharing is best practice in most situations but it is not always possible or appropriate to do so.

Information sharing protocols

An Information Sharing Protocol (ISP) is a signed agreement between two or more organisations relating to a specified information sharing activity. An ISP explains the terms under which the organisations have agreed to share information and the practical steps that need to be taken to ensure compliance with those terms. If there is an ISP applicable to your information sharing situation, you must follow that. ISPs are not required for information sharing. The absence of an ISP should not prevent sharing information.

The Golden Rules[1] for information sharing

Where you are considering sharing information and you do not have the person's consent and there is not an information sharing protocol in place to govern that exchange of information; following the golden rules should ensure that you strike the correct balance between protecting people's privacy and ensuring that fellow practitioners have the information they need to deliver services.

1. Remember that the Data Protection Act is not a barrier to sharing information but provides a framework to ensure that personal information about living persons is shared appropriately.

2. Be open and honest with the person from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.

3. Seek advice if you are in any doubt, without disclosing the identity of the person where possible.

4. Share with consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgment, that lack of consent can be overridden in the public interest. You will need to base your judgment on the facts of the case.

---

[1] The Golden Rules have been copied from "Information Sharing: Guidance for practitioners and managers" published by the Department for Children, Schools and Families, and Communities and Local Government.

5. **Consider safety and well-being:** Base your information sharing decisions on considerations of the safety and well-being of the person and others who may be affected by their actions.

6. **Necessary, proportionate, relevant, accurate, timely and secure:** Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely.

7. **Keep a record** of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

Appendix F: Caldicott principles

1. Justify the purpose(s)

Every proposed use or transfer of 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 identifiable information unless it is absolutely necessary

Identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for subjects to be identified should be considered at each stage of satisfying the purpose(s).

3. Use the minimum necessary identifiable information

Where use of 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 identifiable information should be on a strict need-to-know basis

Only those individuals who need access to 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 identifiable information should be aware of their responsibilities

Action should be taken to ensure that those handling identifiable information are made fully aware of their responsibilities and obligations to respect confidentiality.

6. Understand and comply with the law

Every use of identifiable information must be lawful. Someone in each organisation handling 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

Health and social care professionals should have the confidence to share information in the best interest of their patients within the framework set out by these principles. They should be supported by the policies of their employees, regulators and professional bodies.

Appendix G: Procedure document for NHS Haringey Clinical Commissioning Group and ACS use of Mosaic and for associated common activity

The purpose of this protocol is to enable approved use of Mosaic as a client record tool and authorised information sharing vehicle between London Borough of Haringey in its role as a Council with Social Services Responsibility and NHS Haringey Clinical Commissioning Group.

It is not practical or desirable to create an environment of highly restricted access to information, as this would defeat the information sharing objective, and could increase risk to vulnerable clients. However, there is a need to safeguard against unauthorised use.

It is recognised that staff in both the NHS Haringey Clinical Commissioning Group and LB Haringey are subject to agency confidentiality policies, record keeping policies and policies on use of computers and IT systems, and that breach of these policies and procedures could give rise to invocation of the parent agency's disciplinary procedures.

The Mosaic system provides an audit capability to identify, by user ID, the records accessed and the type of access activity undertaken and date and time of the activity. This would facilitate an underpinning safeguard.

The proposed information sharing protocol is to adopt the convention of an on screen warning note to be created by the person record initiator/owner, where information sharing agreement has not been given by the client/service user. The proposed text is **"WARNING INFORMATION SHARING CONSENT NOT GIVEN – access own agency information only"**, which would be displayed on the front – personal details screen.

The expectation is that workers should seek to get the information sharing agreement signed, and once signed, the warning should be removed.

Additional case note classifications of **"Confidential – NHS case note"; "Confidential LBH case note"** are also proposed.

Control of access to areas of the system and the data will be maintained by the use of 'worker roles' which are assigned to each system user. For example, 'NHS worker' could access episodes which are confidential to NHS staff only. Individual clients, on request from Senior Management, can have access to their records restricted to specified worker roles e.g. 'Child Protection Social Worker'.