Hillingdon
safeguarding
adults board

Hillingdon Safeguarding Adults Board Information Sharing Agreement

2022

Hillingdon
safeguarding
adults board

Contents

1. Introduction 3
2. Scope 3
3. Information Sharing Purposes 4
4. Information to be Shared 4
5. Methods Used for sharing information 6
6. Need to Know 7
7. Legal and regulatory framework 7
8. General guidance 7
9. Information Retention and Destruction 10
10. Security breaches 11
11. Right of Access Request (also known as Subject Access Requests SAR) 12
12. Resolving disputes between parties 12
13. Termination 12
14. Review 13
15. Signatories 14

Appendix 1 15
Appendix 2 16
Appendix 3 17
Appendix 4 18

Hillingdon
safeguarding
adults board

1. Introduction

1.1 The objective of a Safeguarding Adults Board (SAB) as defined by section 43 of the Care Act 2014 is "to help and protect adults in its area...by co-ordinating and ensuring the effectiveness of what each of its members does."

1.2 This Information Sharing Agreement is developed to support Hillingdon SAB and its partners in sharing the right information, at the right time, with the right people. This is fundamental to good practice in safeguarding adults by exercising co-operation across partner organisations and is also underpinned by law.

1.3 The purpose of this document is to:

- **Promote** the safeguarding of adults by the carefully considered sharing of information about identified risks
- **Help** front-line staff adopt a proportionate and consistent approach to balancing the risks of non-disclosure against the infringement of individuals' rights to privacy and confidentiality.

1.4 This agreement is jointly approved by the agencies represented on Hillingdon Safeguarding Adults Board (**see Appendix 1**).

1.5 Hillingdon Safeguarding Adults Board (SAB) recognises the need to provide clear guidance to staff in partner organisations on when and how to share information, in order to both:

a) Prevent abuse or neglect of adults at risk, and
b) Establish facts in order to safeguard and aid the recovery of adults at risk

1.6 This Information Sharing Agreement supersedes any previous SAB Information Sharing Agreement.

1.7 The Data Protection Act (2018) and the principles of the UK General Data Protection Regulation (UK GDPR) provide a legislative framework for the lawful sharing of information and personal data.

2 Scope

2.1 This document does not replace any individual Information Sharing Agreements between partner agencies and this document should be read in conjunction with your own Agency's policies and procedures governing information sharing to safeguard adults at risk. Where any conflict between local procedures and this Information Sharing Agreement is identified, this should be discussed with a senior manager within the Agency concerned and also reported to the Safeguarding Adults Board.

2.2 This Information Sharing Agreement only covers inter-agency sharing of information for the purposes of safeguarding adults. In particular, it does **not** cover information sharing or disclosure in respect of:

- Disclosure between Social Care, Police and Crown Prosecution Service,
- For information-sharing in connection with the Multi-Agency Public Protection Panel or Multi-Agency Risk Assessment Committee (MARAC)
- Disclosure of information in cases of alleged child abuse and linked criminal and care directions hearings

3 Information Sharing Purposes

This document refers to information sharing which may have the following purposes:

3.1 To seek advice about a specific adult safeguarding situation or to establish grounds for an adult safeguarding response.
3.2 To prevent or detect a crime, or support the prosecution of offenders.
3.3 To raise a safeguarding adults concern.
3.4 To safeguard an adult at risk.
3.5 To make a referral to a partner organisation for immediate action to protect an adult.
3.6 To establish the potential need for involvement of partner organisations in adult safeguarding work (enquiry, prosecution or protection arrangements).
3.7 To plan an adult safeguarding enquiry.
3.8 To initiate and conduct an adult safeguarding enquiry.
3.9 To make a referral to organisations for the purposes of requesting or amending services to persons at risk of abuse or neglect.
3.10 To make a referral to organisations for the purposes of requesting or amending services to persons or organisations alleged to have caused harm (also known as "source of risk").
3.11 To notify the Designated Adult Safeguarding Lead about a person in a position of trust who poses a risk to children or adults of abuse or neglect.
3.12 To make a referral to the Disclosure and Barring Service (DBS) or to provide information to the DBS for the purposes of them coming to a barring decision.
3.13 To make a referral, or to provide information, to a professional regulator for the purposes of them coming to a decision.
3.14 To notify the Care Quality Commission who may need to take action relating to a source of risk that is a registered care provider.
3.15 To notify the Charity Commission who may need to take action relating to an organisation alleged to have caused harm (also known as "source of risk") that is a registered charity.
3.16 To notify employers who may need to take action about a member of staff, volunteer or student (paid or unpaid) who is believed to be a source of risk in the course of their work.
3.17 To notify service providers of a risk posed by a service user.
3.18 To inform the development of multi-agency policies and strategies for protecting adults at risk of abuse.
3.19 To monitor and review adult safeguarding concerns and the impact of adult safeguarding policies and procedures, including both the equalities (race,

ethnicity, gender, sexuality, age, disadvantage and disability) impact of the policies and the outcomes for individuals. This may include both quantitative and qualitative information, personal data and special category personal data, the personal views of individuals and expressions of relevant professional opinion.

3.20 To conduct safeguarding adults reviews.

3.21 To deal with complaints, grievances, professional and administrative malpractice.

4. Information to be Shared

4.1 What types of information will be shared?

There are three distinct classifications of data covered by the Data Protection Act (2018): Personal data, Special category data and Criminal Offence data.

4.2 Personal Data includes information relating to a living individual who can be identified directly from the information in question or who can be indirectly identified from that information in combination with other information. Personal data includes identifiers such as names, addresses, dates of birth, NHS or National Insurance numbers. Facial photographs and CCTV footage are also regarded as personal data.

4.3 Special Category Data includes personal data revealing racial or ethnic origins, political opinions, religious or philosophical beliefs and trade union membership. It also includes genetic data and biometric data (where used for identification purposes). In addition, it includes data concerning health and data concerning an individual's sex life and sexual orientation.

4.4 Criminal Offence Data covers a wide range of information about criminal activity, allegations, investigations and proceedings. This includes unproven allegations, information relating to the absence of convictions and personal data of victims and witnesses of crime.

4.5 Information relating to adult safeguarding may involve a wide range of both personal data and special category data, in circumstances relating to many types of abuse and neglect. Further descriptions of types of abuse and neglect can be found within the Care and Support Statutory Guidance (which was issued under the Care Act 2014) at Care and support statutory guidance - GOV.UK (www.gov.uk). Section 14.17 of the Care and Support Statutory Guidance states that Local Authorities are advised not to limit their view of what constitutes abuse or neglect, as they can take many forms and the circumstances of the individual case should always be considered including:

- Physical abuse
- Domestic violence
- Sexual abuse
- Sexual exploitation
- Psychological abuse
- Financial or material abuse

- Modern slavery
- Discriminatory abuse
- Organisational abuse
- Neglect and acts of omission
- Self-neglect

It is impossible to cover all potential scenarios in this Information Sharing Agreement and additional guidance can be found at **Appendix 2.** The guidance is therefore to:

1. Share as much as, but no more than, is necessary.
2. Always document the reasons for sharing Personal data, Special category data and Criminal Offence data.
3. Record why it is believed the data shared is relevant and proportionate.

5. Methods Used for sharing information

5.1 Within the Safeguarding Process, information may be transferred in the following ways:

- Verbally, face to face, in meetings or on the telephone.
- In written communications, (for example, forms, minutes, letters, statements or reports)
- Transferred in hard copy through internal or external mail services.
- Documents transferred on encrypted electronic digital media devices.
- In written information transferred by secure email, or secure file transfer systems.
- Information accessed in situ, via provision of access to organisational databases or records.

5.2 When each of these methods is used, it is essential to consider the safest way to record and mark the information, and to ensure safe transit and delivery. Information should be appropriately secured in transit and transferred by secure encrypted methods.

a) Verbal conversations and interviews should be recorded in a written statement. Care must be taken to record and denote information clearly as fact, statement or opinion and to attribute any statement or opinion to the owner. All information should be recorded in such a way that it can be used as evidence in court, should that be required at a later date.

b) Meetings should be recorded in minutes that are agreed by the delegates present.

c) Written communications containing confidential information should either be transferred in a sealed envelope and addressed by name to the designated person within each organisation. They should be clearly marked "Private & Confidential – to be opened by the recipient only" or alternatively, parties should adhere to their own policy for dealing with external mail.

d) When files are transferred on electronic digital media devices, the files should be encrypted to an appropriate standard, with decryption keys / passwords supplied separately.

e) Data is to be sent securely and received electronically to ensure there is an audit trail. Any e-mail communication will be by way of secure, appropriate and approved methods. The sharing of any data must be done via secure methods by email which should be industry standard encryption, as approved by your organisation.

5.3 The onus is on the organisation sending the information to ensure that:

- Information is transferred securely
- The chosen method is acceptable to and workable by the recipient
- Information has reached the required recipient

5.4 In the event that a recipient receives information by an unsecured route, it is the responsibility of the recipient to advise the sender and agree a secure route for future transfers of information. This can include the use of industry standard encryption, as approved by your organisation.

6. Need to Know

6.1 Key roles of individuals within the Safeguarding process will govern whether they need to know information about adults at risk, alleged sources of risk, witnesses and other information pertaining to incidents.

6.2 In addition to those raising or responding to safeguarding adults concerns, other people who may contribute and receive information include other staff and managers, volunteers, family members, carers and witnesses. These people may be invited to contribute to strategy discussions or meetings, enquiries and case conferences and reviews.

6.3 At all times, it is essential to be certain of the reasons why an individual or attendees at a meeting need access to the information. It is important to consider whether it is necessary for this individual or attendee at a meeting to be aware of this information in order to conduct the enquiry or to safeguard an adult at risk or witness.

6.4 Where an enquiry involves more than one adult at risk, it may be necessary to partition meetings so that contributors can be invited only for specific items, based on their need to know.

7. Legal and regulatory framework

7.1 Information-sharing is related to a number of different pieces of legislation:

- Local authority responsibilities for sharing information under the Care Act 2014
- The common law duty of confidentiality
- The Human Rights Act 1998, Article 8 (the right to respect for private life)
- The Data Protection Act 2018
- The Crime and Disorder Act 1998
- The Mental Capacity Act 2005

7.2 In addition to this there are a number of professional's codes of conduct which identify people's right to privacy and confidentiality.

7.3 All staff and volunteers should be familiar with their internal safeguarding procedures for raising concerns. Should they have a safeguarding concern they should discuss this with their line manager. They can also contact Hillingdon Social Care services for advice, without necessarily giving an individual's personal details, if they are not sure whether a safeguarding referral would be appropriate.

7.4 While it is regarded as good practice for staff and volunteers to seek consent from individuals before sharing their personal data and/or special category data, consent is not the basis for sharing information because sharing information to safeguard adults at risk, or to cooperate with other individuals or organisations that are working to protect adults at risk, is a Local Authority duty under sections 6, 7 & 45 of the Care Act 2014.

7.5 In the event that an organisation declines to share information considered necessary to enable the SAB to exercise its functions, consideration should be given to whether the concern warrants the Board exercising Section 45 of the Care Act 2014.

7.6 A 'Supply of Information' request made by the SAB under section 45 of the Care Act 2014 to any person "to supply information to it, or to some other person specified in the request", the person to whom the request is made must comply with the request, subject to certain prescribed conditions being satisfied. The conditions are set out in Appendix 3.

7.7 Such supply of information requests may concern, but are not necessarily limited to, Safeguarding Adults Reviews and the undertaking of safeguarding enquiries, and are only for the purpose of enabling or assisting the SAB to exercise its functions.

7.8 Section 14 of the Care and Support Statutory Guidance sets out the following guidance at paragraph 14.186:

An SAB may request a person to supply information to it or to another person. The person who receives the request must provide the information to the SAB if:

- the request is made in order to enable or assist the SAB to do its job
- the request is made of a person who is likely to have relevant information and then either:

- the information requested relates to the person to whom the request is made and their functions or activities
- the information requested has already been supplied to another person subject to an SAB request for information

7.9 Requests for the SAB to exercise Section 45 of the Care Act 2014 must be made in writing to the Chair of the SAB by the organisation's Board Member or Deputy, detailing how the relevant criteria is met. Wherever practicable, the Chair of the SAB will seek the views of statutory members of the Board, before reaching a decision as to whether to exercise Section 45 of the Care Act 2014. This may not always be possible for example, where such a delay would place an individual at further risk.

7.10 Article 6 of the UK GDPR stipulates that you must have a valid lawful basis in order to process Personal Data. The lawful bases identified here are as follows:

- Article 6(1)(a) - the individual has given clear consent to process their personal data for a specific purpose;
- Article 6(1)(c) - processing is necessary for compliance with a legal obligation;
- Article 6(1)(d) – processing is necessary to protect someone's life (vital interest);
- Article 6(1)(e) - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

7.11 Article 9 of the UK GDPR stipulates that you must also have a condition for processing Special Category Data such as health. The conditions for processing identified here are as follows:

- Article 9(2)(a) - explicit consent from the data subject
- Article 9(2)(c) – processing is necessary to protect the vital interest of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
- Article 9(2)(h) - health or social care (with a basis in law) and the associated condition in paragraph 2(d) and 2(e) in Part 1 of Schedule 1 of Data Protection Act 2018 for the provision of healthcare or treatment and the provision of social care.
- Article 9(2)(g) – reasons of substantial public interest (with a basis in law) and the specific substantial public interest conditions 10 (preventing or detecting unlawful acts) and 18 (safeguarding individuals at risk) in Part 2 of Schedule 1 of the Data Protection Act 2018.

7.12 The signatories to this Information Sharing Agreement undertake that where Criminal Offence Data is processed, there must be both a lawful basis under Article 6 and either legal authority or official authority for the processing under Article 10 of the UK GDPR. In addition, a specific condition in Schedule 1 of the Data Protection Act 2018 and additional safeguards in this Act must be met.

7.13 In addition, the parties should have regard to the Human Rights Act 1998, the Common Law Duty of Confidentiality and the Caldicott principles. The Caldicott Principles are set out at The Caldicott Principles - GOV.UK (www.gov.uk) and all

parties must adhere to these principles when sharing patient health data.

7.14 It is necessary for The London Borough of Hillingdon Adult Social Care services to share the personal information outlined within this agreement in order that the Local Authority fulfils its statutory duties under the Care Act 2014. Statutory guidance is available on all parts of the Care Act 2014.

7.15 Each signatory will be deemed as a Data Controller for information they collected to fulfil its statutory functions, and as such will be responsible for its own information governance compliance including identifying lawful bases for the sharing of Personal Data, Special Category Data and Criminal Offence Data.

8. General guidance

8.1 If consent it obtained, where appropriate, it should be recorded using approved consent documentation and/or information systems. Where it is not possible to obtain consent, this could be because:

- the individual does not have the mental capacity to consent
- it may not be safe to seek consent
- it may not be possible to seek consent for some other reason

8.2 In cases where it has not been possible to seek or obtain consent, staff or volunteers should always record the justification for sharing the information, and how this decision was arrived at.

8.3 If the individual does not have the mental capacity to consent, staff or volunteers should record this using their agency's Mental Capacity Assessment recording tool, and record their decisions to share information using their agency's Best Interests Decision recording tool.

8.4 The seven golden rules to sharing information is provided in **Appendix 4** as guidance only. For further advice on justifiable grounds for sharing information, contact your organisation's Data Protection specialist or Caldicott Guardian.

9. Information Retention and Destruction

9.1 The Data Protection Act 2018 requires that personal data is not retained for longer than is necessary. Partner organisations may have their own organisational, legal or procedural requirements for records retention and disposal. These retention schedules should be observed and applied at all times.

9.2 Where no such organisational procedure exists, it is essential to keep pertinent information as long as there continues to be a need for protection arrangements, to ensure that protection arrangements are not compromised and equally that such information is securely disposed of when no longer required.

10. Security breaches

10.1 A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

10.2 The parties to this agreement are responsible for notifying the other party in writing in the event of a personal data breach within 24 hours of becoming aware of the event.

10.3 The parties to this agreement will discuss and agree the next steps relating to the incident, taking specialist advice where appropriate including from their respective Data Protection Officer. Such arrangements will include (but will not be limited to) containment of the incident and mitigation of any ongoing risk, recovery of the information, and assessing whether the Information Commissioner's Office and / or the data subjects will be notified. The arrangements may vary in each case, depending on the sensitivity of the information and the nature of the personal breach.

10.4 Where appropriate and if relevant to the incident, disciplinary misconduct action and/or criminal proceedings will be considered.

10.5 The parties shall indemnify and keep indemnified each other against all losses, claims, damages, liabilities, fines, sanctions, interest, penalties, costs charges and expenses including legal fees and costs at any time incurred or suffered by a party to this Agreement arising on or in connection with any breach by a party of its obligations under this Information Sharing Agreement. Provided that such indemnity may only be invoked in the circumstances set out in sub-clauses 10.5.1 to 10.5.3 below.

10.5.1 The party seeking the indemnity may only seek to enforce it against the party that supplied or misused the information in accordance with this Agreement.

10.5.2 The party claiming the benefit of the indemnity has notified the party against whom it intends to invoke the indemnity within 14 days of any third party action claim or demand ("the claim") and thereafter the parties shall consult as to how the party against whom the claim has been made ("the defendant") shall proceed in respect of such claim.

10.5.3 The party seeking to invoke the indemnity may not do so if it has made or makes any admission which may be prejudicial to the defence of the action, claim or demand.

10.6 The sharing of data may be suspended pending resolution in accordance with the terms of this agreement.

10.7 The Parties shall comply with the provisions of the Data Protection Act 2018, UK

General Data Protection Regulation (UK GDPR) and any other relevant data protection law in force as applicable to this agreement.

10.8 Any issues concerning compliance with security measures will form part of the review of this agreement

11. Right of Access Request (also known as Subject Access Requests (SAR))

11.1 It is the responsibility of each party to this agreement as a data controller of the personal data shared under this agreement, to deal with a subject access request made by a data subject in exercise of the data subject's rights under UK GDPR and the Data Protection Act 2018. This is in accordance with the statutory obligations of that data controller.

11.2 The party receiving the SAR should notify the other parties within five working days of receiving a request from a Data Subject to have access to that person's personal data (including special categories of personal data and sensitive processing); or a complaint or request relating to the parties obligations under data protection legislation.

11.3 The party receiving the SAR must contact the other parties to determine whether they wish to claim an exemption or if they have any objections under the provisions of the relevant Act before any disclosure takes place. Data should not be disclosed that would compromise an investigation or proceedings.

12. Resolving disputes between parties

12.1 Any issues or disputes that arise as a result of the data sharing covered by this agreement must be directed to the signatory to this agreement. Each party will be responsible for escalating the issue as necessary within their organisations.

12.2 Where a problem arises it should be reported as soon as possible. Should the problem be of an urgent nature, it must be reported by phone immediately to the signatories to this Agreement and followed up in writing the same day. If the problem is not of an urgent nature it can be reported in writing within 24 hours of the problem occurring.

13. Termination

13.1 All parties to this agreement reserve the right to terminate this Data Sharing Agreement with one months' notice.

13.2 In the event of a significant personal data breach or other serious breach of the terms of this Information Sharing Agreement by any party, the Information Sharing Agreement will be terminated or suspended immediately without notice.

14. Review

14.1 Should any member of staff or volunteer working for a partner organisation feel that the Information Sharing Agreement is not being complied with, this should be communicated to their organisation's representative on the Hillingdon Safeguarding Adults Board, who will in turn follow this up with their counterparts and Data Protection leads in the Member organisation.

14.2 This agreement will commence on the date that the Information Sharing Agreement is signed by all the Parties. A review will take place on an annual basis from the the commencement date and thereafter on an annual basis.

Hillingdon
safeguarding
adults board

15. Signatories

Signatories to this Hillingdon Safeguarding Adults Board Information Sharing Agreement

By signing below, the partner organisation agrees they will comply with the terms set out in this SAB Information Sharing Agreement, the UK GDPR, Data Protection Act 2018 and any other relevant legislation.

Signature: .....

Full name of the person signing Bukky Junaid

Job Title Interim Head of Service Safeguarding Adults, Adults LADO and Principal Social Worker for Adults

For and on behalf of (Organisation) London Borough of Hillingdon

Date 18 March 2022

Hillingdon safeguarding adults board

15. Signatories

Signatories to this Hillingdon Safeguarding Adults Board Information Sharing Agreement

By signing below, the partner organisation agrees they will comply with the terms set out in this SAB Information Sharing Agreement, the UK GDPR, Data Protection Act 2018 and any other relevant legislation.

Signature:  .....

Full name of the person signing ..... Dr Sanjay Gautama .....

Job Title ..... North West London ICS / CCG CCIO and Caldicott Guardian .....

For and on behalf of (Organisation) ..... NWL CCG .....

Date..... 25/03/22 .....

Hillingdon safeguarding adults board

15. Signatories

Signatories to this Hillingdon Safeguarding Adults Board Information Sharing Agreement

By signing below, the partner organisation agrees they will comply with the terms set out in this SAB Information Sharing Agreement, the UK GDPR, Data Protection Act 2018 and any other relevant legislation.

Signature: .....

Full name of the person signing Mustafa Khan

Job Title Deputy Director, Passenger Operations

For and on behalf of (Organisation) Border Force

Date 11/04/2022

Hillingdon safeguarding adults board

15. Signatories

Signatories to this Hillingdon Safeguarding Adults Board Information Sharing Agreement

By signing below, the partner organisation agrees they will comply with the terms set out in this SAB Information Sharing Agreement, the UK GDPR, Data Protection Act 2018 and any other relevant legislation.

Signature: 

Full name of the person signing Glen Nicolaides

Job Title Station Commander Hillingdon Fire Station

For and on behalf of (Organisation) London Fire Brigade

Date 10th March 2022

Hillingdon
safeguarding
adults board

15. Signatories

Signatories to this Hillingdon Safeguarding Adults Board Information Sharing Agreement

By signing below, the partner organisation agrees they will comply with the terms set out in this SAB Information Sharing Agreement, the UK GDPR, Data Protection Act 2018 and any other relevant legislation.

Signature: .....
.....

Full name of the person signing ALASTAIR PETER PENMAN
.....

Job Title .....Hillingdon Borough Director
.....

For and on behalf of (Organisation) ....Central and North West London NHS Foundation Trust .....

Date.....18/3/22.....
.....

Hillingdon safeguarding adults board

15. Signatories

Signatories to this Hillingdon Safeguarding Adults Board Information Sharing Agreement

By signing below, the partner organisation agrees they will comply with the terms set out in this SAB Information Sharing Agreement, the UK GDPR, Data Protection Act 2018 and any other relevant legislation.

Signature: .....

Full name of the person signing .....JAN M ELLIOTT.....

Job Title ..LEAD - CHILDREN & YOUNG PEOPLE'S SERVICE & SAFEGUARDING CHAMPION

For and on behalf of (Organisation) ...THE CLEMENTINE CHURCHILL HOSPITAL - PART OF CIRCLE HEALTH SA...

Date.....10-3-2022.....

Hillingdon safeguarding adults board

15. Signatories

Signatories to this Hillingdon Safeguarding Adults Board Information Sharing Agreement

By signing below, the partner organisation agrees they will comply with the terms set out in this SAB Information Sharing Agreement, the UK GDPR, Data Protection Act 2018 and any other relevant legislation.

Signature: .....

Full name of the person signing Daniel West .....

Job Title Managing Director .....

For and on behalf of (Organisation) Healthwatch Hillingdon .....

Date 23/03/2022 .....

Hillingdon safeguarding adults board

15. Signatories

Signatories to this Hillingdon Safeguarding Adults Board Information Sharing Agreement

By signing below, the partner organisation agrees they will comply with the terms set out in this SAB Information Sharing Agreement, the UK GDPR, Data Protection Act 2018 and any other relevant legislation.

Signature: .....

Full name of the person signing ..... SAS HUSSAIN .....

Job Title ..... DETECTIVE CHIEF INSPECTOR .....

For and on behalf of (Organisation) ..... METROPOLITAN POLICE .....

Date ..... 19/04/22 .....

Hillingdon safeguarding adults board

15. Signatories

Signatories to this Hillingdon Safeguarding Adults Board Information Sharing Agreement

By signing below, the partner organisation agrees they will comply with the terms set out in this SAB Information Sharing Agreement, the UK GDPR, Data Protection Act 2018 and any other relevant legislation.

Signature: 

Full name of the person signing: Jason Seez

Job Title: Director of Strategy & Senior Information Risk Owner

For and on behalf of (Organisation): The Hillingdon Hospitals NHS Foundation Trust

Date.9th March 2022

Hillingdon safeguarding adults board

15. Signatories

Signatories to this Hillingdon Safeguarding Adults Board Information Sharing Agreement

By signing below, the partner organisation agrees they will comply with the terms set out in this SAB Information Sharing Agreement, the UK GDPR, Data Protection Act 2018 and any other relevant legislation.

Signature: .....

Full name of the person signing Ayodeji Ogunyemi

Job Title Head of Service - Ealing and Hillingdon

For and on behalf of (Organisation) The Probation Service

Date 15th March 2022

Hillingdon safeguarding adults board

Appendix 1

Hillingdon Safeguarding Adults Board members

London Borough of Hillingdon
North West London Clinical Commissioning Group
Border Force
London Fire Brigade
Central and North West London NHS Foundation Trust.
BMI Healthcare
Healthwatch Hillingdon
Metropolitan Police Service
The Hillingdon Hospitals NHS Foundation Trust
Probation Service

Hillingdon
safeguarding
adults board

Appendix 2

Additional guidance

Department of Health: Care and Support Statutory Guidance – issued under the Care Act 2014 (available at Care and support statutory guidance - GOV.UK (www.gov.uk)

ICO Data Sharing Code of Practice for Sharing of Personal Data
(available at Data sharing: a code of practice | ICO)

Information Sharing: Guidance for Practitioners and Managers (Social Care Institute for Excellence) as at January 2019
(available at http://www.scie.org.uk/care-act-2014/safeguarding-adults/sharing-information/seven-golden-rules.asp)

Hillingdon safeguarding adults board

Appendix 3

Section 45 of Care Act 2014

45. Supply of information

(1) If an SAB requests a person to supply information to it, or to some other person specified in the request, the person to whom the request is made must comply with the request if—

(a) conditions 1 and 2 are met, and

(b) condition 3 or 4 is met.

(2) Condition 1 is that the request is made for the purpose of enabling or assisting the SAB to exercise its functions.

(3) Condition 2 is that the request is made to a person whose functions or activities the SAB considers to be such that the person is likely to have information relevant to the exercise of a function by the SAB.

(4) Condition 3 is that the information relates to—

(a)the person to whom the request is made,

(b) a function or activity of that person, or

(c) a person in respect of whom that person exercises a function or engages in an activity.

(5) Condition 4 is that the information—

(a) is information requested by the SAB from a person to whom information was supplied in compliance with another request under this section, and

(b) is the same as, or is derived from, information so supplied.

(6) Information may be used by the SAB, or other person to whom it is supplied under subsection (1), only for the purpose of enabling or assisting the SAB to exercise its functions.

Appendix 4

The seven golden rules to sharing information

This is derived from Information Sharing: Guidance for Practitioners and Managers [1] (HM Government, January 2019) and is available at http://www.scie.org.uk/care-act-2014/safeguarding-adults/sharing-information/seven-golden-rules.asp.

1. **Remember that the UK General Data Protection Regulation (UK GDPR) 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 (and/or their family where appropriate) 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 judgement, that lack of consent can be overridden in the public interest. You will need to base your judgement on the facts of the case.

5. **Consider safety and wellbeing:** base your information-sharing decisions on considerations of the safety and wellbeing 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.