

Public Service

 **ombudsman**

Information Sharing Protocol

V1.3 March 2024

1 Purpose

- 1.1 This information sharing protocol provides clarity on when information can be shared with another public body or organisation within Great Britain and Northern Ireland.
- 1.2 This protocol has been designed to provide guidance for colleagues who are seeking to share information with other organisations, to enable them to do so safely and appropriately.
- 1.3 The protocol will ensure all stakeholders have a shared understanding of what is required to progress through each key stage of information sharing.

2 Not in Scope

- 2.1 This information sharing protocol does not apply to sharing information with private individuals or private firms or agencies acting on their behalf e.g. solicitors.
- 2.2 This information sharing protocol is limited to personal data. Information about payments and financial transactions, for example, is not covered. If you are considering the disclosure of non-personal data, please contact the information rights team in the first instance who will review and evaluate on a case-by-case basis.
- 2.3 Anonymised data i.e. data from which a person cannot be identified is not covered by this protocol as this information is not personal data and 2.2 applies.
- 2.4 The provision of material evidence to complainants and the fulfillment of statutory information rights such as subject access requests and freedom of information requests are not covered within this protocol. For more information about this contact the information rights team.

3 When is an information sharing agreement needed?

- 3.1 Not all instances of sharing will require a formal information sharing agreement. There are no hard and fast rules but in general, an information sharing agreement is only necessary when:
 - The information being shared is high-risk as determined by the Data Protection Impact Assessment (DPIA) screening tool;
 - Information will be shared regularly;
- 3.2 Arrangements need to be put in place to control what happens to the information after it has been shared;
- 3.3 Information sharing is necessary to enable business critical processes;

- 3.4 One or more organisations are involved;
- 3.5 The information sharing relies on specific technologies that require maintenance and monitoring.
- 3.6 Examples of when an information sharing agreement have been required include:
- The regular sharing of complainant information with LGSCO for the purposes of joint investigation;
 - Sharing final reports with organisations such as CQC;
 - Receiving automated patient and demographic information from the NHS.
- 3.7 An information sharing agreement will usually not be necessary when the sharing is expected or specified in law. Examples include:
- Caseworker calling 999 to report someone being harmed;
 - We share information with an organisation under investigation;
 - We supply information for a formal inquiry e.g. infected blood inquiry;
 - We provide tax information to HMRC.

4 Content

- 4.1 The personal information held and handled by us is not 'our' information. We control how it is used, but we do not 'own' this personal information. Even though our legislation allows us to investigate privately, we must uphold the information rights of the people whom the information relates to.
- 4.2 We can uphold information rights and still choose to share personal information without consent. The law, in certain circumstances, allows us to share information without asking permission such as when it's necessary to fulfil a contract or for a legitimate business purpose but please seek advice from the Data Protection Officer (DPO) before doing so.
- 4.3 This does not apply if you suspect that someone is at imminent risk of harming themselves or others in which case call 999. If someone threatens to harm themselves or others, please refer the matter to Information Access and Assurance by [Helphub](#).
- 4.4 You must ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is accurate and up to- date, is shared in a timely fashion, and is shared securely.

- 4.5 Remember that data protection is not about saying 'no'. The UK General Data Protection Regulation (GDPR), Data Protection Act 2018 and human rights law provide a framework to enable personal information about living individuals to be shared appropriately.
- 4.6 Being transparent means being open and honest with the individual (and/or their family or representatives where appropriate) from the outset. In our privacy notices we define why, what, how and with whom information will, or could be shared.
- 4.7 You must seek advice from the Data Protection Officer, and the information rights team before sharing personal information with any external organisation.
- 4.8 This includes information obtained during the course of an investigation. This is so that we can safeguard our right to investigate in private.
- 4.9 Less is more when it comes to information sharing. If you can, share information without disclosing the identity of the individual or other information that would allow someone else to identify them.
- 4.10 Consider whether you can anonymise the information. This means removing or obfuscating information that would allow an individual to be identified or would allow someone else to infer private information about a person. Anonymisation can be simple or complex so please notify Information Access and Assurance of your intentions so that we can support you through this process.
- 4.11 Under the UK GDPR and Data Protection Act 2018 you may share personal information without consent if, in your judgement, there is a **lawful basis** to do so, such as where safety may be at risk. If there is no imminent risk of harm, then please consult the [Disclosing concerns about patients policy](#) or contact the DPO for advice.
- 4.12 When considering if there is a need to share information, you will need to base your judgement on the facts of the case. When you are sharing personal information from someone, be clear of the legal basis upon which you are doing so, and whether we have consent to do so. Please contact the DPO for advice.
- 4.13 In considering whether to share information, it is important to consider whether the safety and wellbeing of the individual whose information it is, may be impacted or compromised by sharing their information. Please contact the DPO for advice.
- 4.14 We must record decision making. The Information Rights Team will record the details of information sharing agreements in the information sharing register once the agreements have been finalised and signed. Prior to the agreement being completed, please keep a local record of emails, process maps and other documents relating to the development of the information sharing agreement until informed that these are no longer necessary.

5 Content

- 5.1 If you have a valid reason, you can share personal data with another public sector organisation.
- 5.2 The examples listed below are intended to illustrate each lawful basis. Not all of these will apply to sharing information with other public sector organisations.
- 5.3 Before you do this, you need to determine what this valid reason or 'lawful basis' is. The lawful basis that's right for you to be able to share information will depend on the reason you want or need to share the data. These bases are:

✓ **Consent**

The individual has given clear consent for us to share their personal data for a specific purpose.

Examples

- Following media enquiries about an anonymised case study, we ask the complainant whether they consent to being contacted by journalists.
- A member of the public submits a complaint covering both health and social care organisations. We ask for their consent to refer the complaint to the joint Public Service Ombudsman/LGSCO working team, which operates under the LGSCO.

✓ **Contract**

Sharing information is necessary to fulfil a contract between us and the individual, or because the individual has asked us to take specific steps before entering into a contract.

Example

- We share information about an employee's needs with a provider of assistive technology solutions to enable that employee to continue working.

✓ **Legal Obligation**

Sharing information is necessary for us to comply with a legal requirement, excluding contractual obligations.

Example

- We provide National Insurance numbers and pay information to HM Revenue & Customs (HMRC) to meet tax and payroll obligations.

✓ Vital Interests

Sharing information is necessary to protect the life or physical safety of an individual.

Example

- We report a complainant to the police after they threaten the life of an employee. Contact details, location information, and other relevant personal data may be shared where necessary to assist the police in locating the individual.

✓ Public Task

Sharing information is necessary for us to perform a task carried out in the public interest or in the exercise of its official functions, where there is a clear legal basis.

Examples

- We share relevant historic records from its archives with a statutory inquiry, such as the Infected Blood Inquiry.
- We share complaint information with the organisation being complained about to enable that organisation to respond, supporting our statutory functions.

✓ Legitimate Interests

Sharing information is necessary for our legitimate interests, or those of a third party, provided these interests are not overridden by the individual's rights and freedoms.

Example

- We share complainants' contact details with a survey provider acting on its behalf to measure customer service performance. Individuals can opt out of receiving survey requests, reflecting the safeguards that apply when relying on legitimate interests.

6 Decision Making

- 6.1 You should begin by using the screening tool on HelpHub to check if you need to complete a Data Protection Impact Assessment (DPIA). The DPIA is a robust risk assessment that evidence that we have considered the implications of information sharing.
- 6.2 This screening tool is intended to help you consider whether a DPIA is required. When complete, this must be returned to the Data Protection Officer ++dpo@ombudsman.org.uk

- 6.3 If the screening tool indicates that you do not need to complete a DPIA, then you can proceed as the information is low risk and unlikely to cause harm to anyone's information rights.
- 6.4 If, however, the screening tool recommends a full DPIA, then this must be completed. You are likely to have to complete a DPIA if the information sharing concerns special category data, i.e. extremely sensitive information such as medical records.

7 When can I share special category data?

7.1 The GDPR defines special category data as:

- personal data revealing racial or ethnic origin.
- personal data revealing political opinions.
- personal data revealing religious or philosophical beliefs.
- personal data revealing trade union membership.
- genetic data.
- biometric data (where used for identification purposes).
- data concerning health.
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

7.2 Data protection law applies to any personal data we hold. Where special category data is concerned, even stronger rules apply. This is because the special categories refer to personal information that could cause significant harm, such as discrimination or physical danger, if it was misused.

7.3 If you are considering sharing any special category data, the Information Rights team will work with you to determine which of the stronger conditions laid out in law would apply.

8 Sharing Information Securely

- 8.1 Information must be shared securely. For small volumes or infrequent sharing, you may use encrypted email (egress). For all other information sharing proposals, submit a request to [Helphub](#). Digital Services will then advise appropriate options based on your requirements.
- 8.2 The security approach will flex as appropriate. Factors to consider include:
- The sensitivity and volume of the information.
 - The security expertise, maturity, and credibility of the recipient organisation(s).
 - The novelty and complexity of the technology involved.

9 Information Sharing Agreement

- 9.1 All parties to the information sharing must sign an information sharing agreement. These are usually public documents, published online. We have a standard template you should use.

10 Review of Information Sharing Agreements

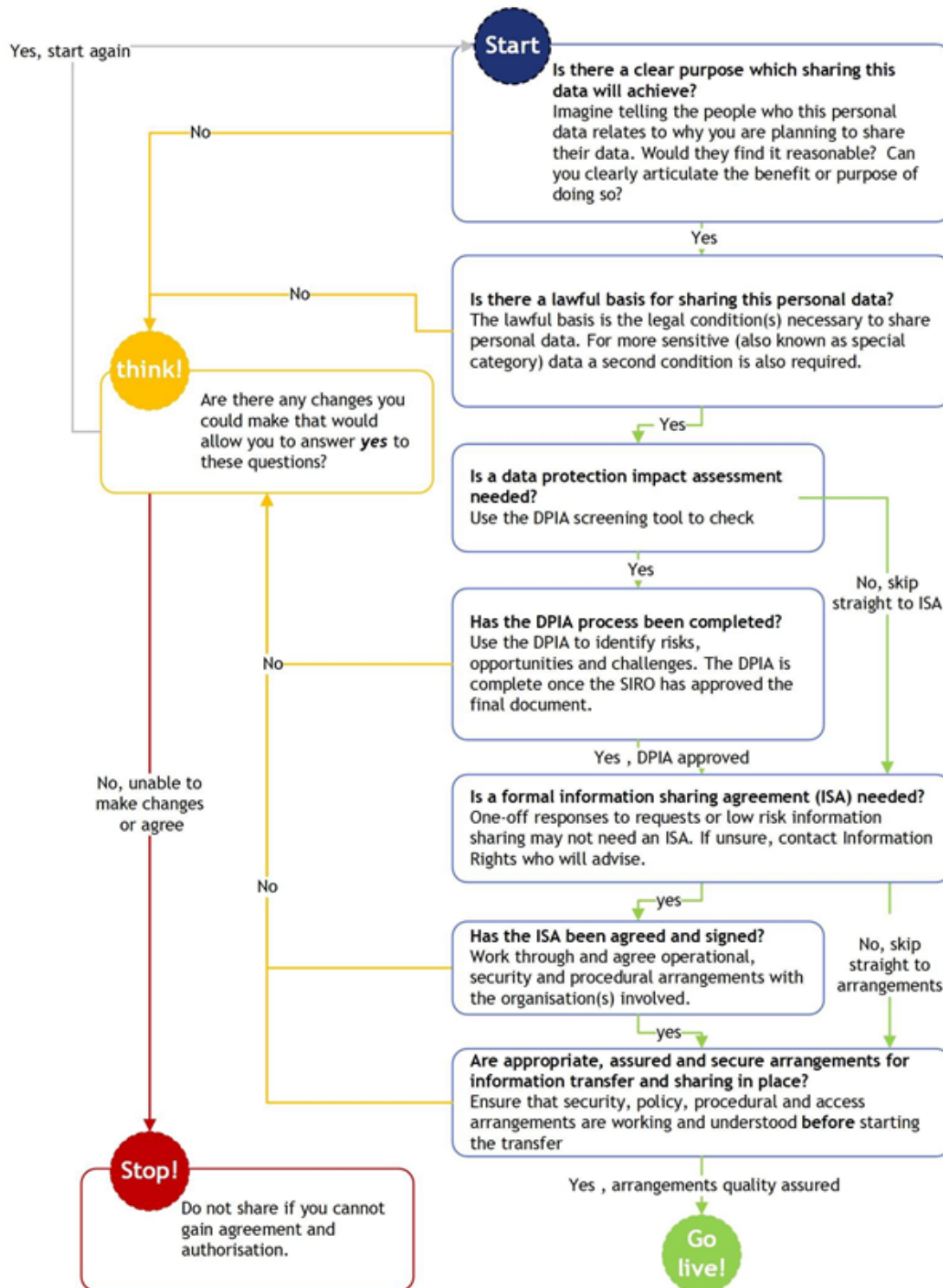
- 10.1 The schedule for reviewing information sharing agreements is as follows.

Time after launch	Key checks
1 month	• Is the data received? • Is it secure? • Is it adequate, limited, and relevant for the purpose?
3 months	• Is it secure? (this may be a good opportunity to conduct technical security testing e.g. penetration tests) • Is it adequate, limited, and relevant for the purpose?

6 months	• Is it adequate, limited, and relevant for the purpose? • Are the expected benefits being realised?
12 months and annually thereafter	• Is the data received? • Is it secure? • Is it adequate, limited, and relevant for the purpose? • Are the expected benefits being realised? • Are agreed retention and destruction actions being carried out appropriately? • Does the information sharing agreement need to be refreshed and/or resigned?

11 Information Sharing Flowchart

Contact information rights for advice and support at any stage of this process



Version control

Date	Version	Amends	Owner of amends
19 Jan 2021	0.1	Draft	James Smuts, Karl Quinn, Mike Avery
25 Jan 2021	0.2	Draft Review	Kate Eisenstein, Andy Medlock
29 Jan 2021	1.0	Final Draft	Gill Kilpatrick, Bipon Bhakri, Stuart Ogden
5 Feb 2021	1.1	Minor updates	Michael Avery
19 July 2023	1.2	Minor updates	Alex Daybank
31 Mar 2025	1.3	Minor updates to team names and links	Alex Daybank