Parliamentary and Health Service Ombudsman

Information Sharing Protocol

Version 1.2 | July 2023

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 across PHSO 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 Out of 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, are 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 these contact the information rights team.

3 When is an information sharing agreement necessary?

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;
- arrangements need to be put in place to control what happens to the information after it has been shared;
- the information sharing is necessary to enable business critical processes;
- one or more organisations are involved;
- the information sharing relies on specific technologies that require maintenance and monitoring.

3.2 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.

3.3 An information sharing agreement will usually not be necessary when the sharing is expected or specified in law. Examples include:

- PHSO caseworker calling 999 to report someone being harmed;
- PHSO shares information with an organisation under investigation;
- PHSO supplies information to a formal inquiry e.g. infected blood inquiry;
- PHSO provides tax information to HMRC.

4 Principles of good information sharing

4.1 The personal information held and handled by PHSO 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 in private, 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 Data, Security and Privacy 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 PHSO's 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 the information rights team 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 PHSO has 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 PHSO 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 Lawful bases for sharing personal information

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 PHSO to share their data for a specific purpose.

Example: Following media enquiries into an anonymised case study, PHSO asks the complainant if they consent to being contacted by journalists.

Example: A member of the public complains to PHSO. Their complaint covers both health and social care organisations. PHSO asks them for their consent to refer their complaint to the PHSO/LGSCO joint working team which operates under the LGSCO.

✓ **Contract**: sharing information is necessary for a contract PHSO have with the individual or because they have asked you to take specific steps before entering into a contract.

Example: PHSO shares information about an employee's needs with a company providing assistive technology solutions to enable that employee to continue to work.

✓ **Legal obligation**: sharing is necessary for PHSO to comply with the law (not including contractual obligations).

Example: PHSO provides national insurance numbers and details of pay to HMRC to comply with tax regulations.

✓ **Vital interests:** sharing this information is necessary to protect someone's life.

Example: PHSO reports a complainant to the police after they threaten the life of an employee. PHSO will also share contact, location, and other personal information as necessary to support the police in locating the offender.

✓ **Public task**: Sharing information is necessary for PHSO to perform a task in the public interest or conduct our official functions, and the task or function has a clear basis in law.

Example: PHSO shares appropriate, historic information from our archives with a formal inquiry, such as the Infected Blood Inquiry.

Example: PHSO shares complaint information with the organisation being complained about to enable that organisation to respond and hence achieve our statutory function.

✓ **Legitimate interests**: sharing information is necessary for PHSO's legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Example: PHSO shares complainants' contact information with a survey company operating on our behalf to assess our customer service performance. People may choose to 'opt-out' when legitimate interest is used hence why

complainants can ask not to be contacted by the survey company.

6 Decision making

6.1 You should begin by using the screening tool to check if you need to complete a Data Protection Impact Assessment (DPIA). The DPIA is a robust risk assessment that evidences that PHSO has considered the implications of the 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 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 PHSO holds. 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 condition 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 the ICT helphub. ICT 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 and credibility of each organisation the information is to be shared with.
- the novelty 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. PHSO has a template you should use linked to this policy.

10 Review of information sharing agreements

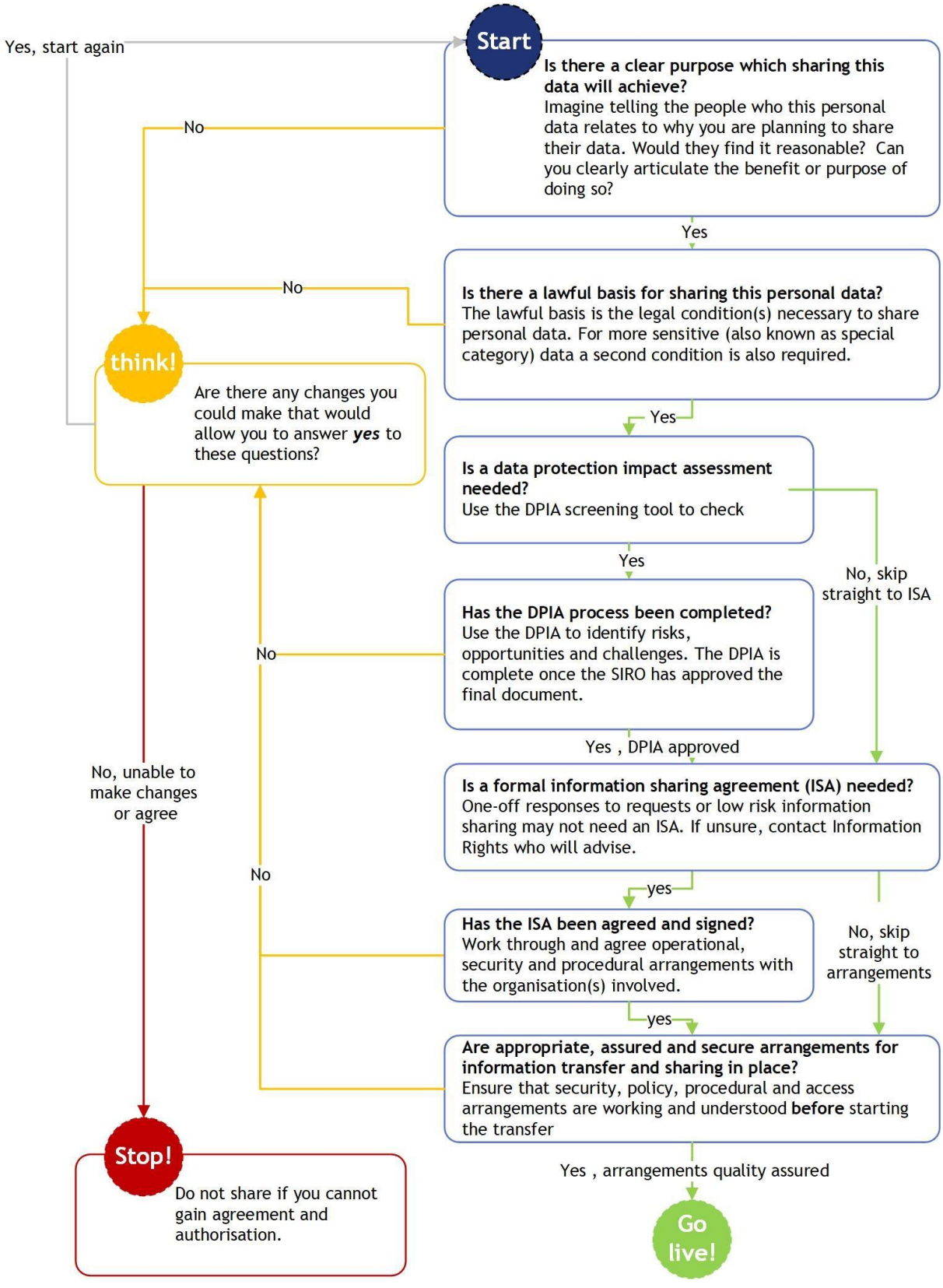
10.1 The schedule for reviewing information sharing agreements is as follows.

Time after launch	Key checks
1 month	• Is the data received? • Is it secure? • Is it adequate, limited, and relevant for the purpose?

Time after launch	Key checks
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



12 Version control

Version	Date	Author	Reviewed by	Authorised by
0.1	19/1/2021	Angharad Jackson	[redacted]	
0.2	25/1/2021	Angharad Jackson	Kate Eisenstein, Andy Medlock	
1	29/01/2021	Angharad Jackson	Gill Kilpatrick, Bipon Bhakri, Stuart Ogden	Gill Kilpatrick
1.1	5/2/2021	Angharad Jackson	[redacted]	
1.2	19/07/2023	Angharad Jackson	Alex Daybank	