How to Document Your Data Processing

Why do I need to do this?
It is a requirement of the Data Protection Act (1998) that all personal data has a legal basis for being shared. The General Data Protection Regulations (GDPR) require that this is documented under the principle of accountability. This document must be made available to the Information Commissioner’s Office (ICO) – the regulator for data protection - on request.

Having a record not only fulfils legal requirements, but also helps with subject access requests – it’s easier to source data when you know where it’s kept – and the information recorded will also form the basis of your privacy notice.

Step One – what do I have?

a) As a first step you should do an audit of what personal data you keep and where it is stored. For example, care records are stored in this room, employee bank details are stored in the payroll system etc. These different types of data are called information assets and you can keep a record of these assets in an information asset register (IAR). We have provided a template.

Personal data is any kind of data relating to an individual who can be identified.

b) Once you know what personal data you have, then consider whether it is special category.

Special category data is:

<table>
<thead>
<tr>
<th>Racial or ethnic origin data</th>
<th>Genetic data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Political opinions</td>
<td>Biometric data (for uniquely identifying someone)</td>
</tr>
<tr>
<td>Religious or philosophical belief(s)</td>
<td>Health data (this includes data used for social care e.g. care plans)</td>
</tr>
<tr>
<td>Trade union membership</td>
<td>Data concerning someone’s sex life or sexual orientation</td>
</tr>
</tbody>
</table>

c) You then need to consider what security procedures you use to protect this data e.g. locked cabinets, passwords, etc.

Step Two - Where is it from and where does it go?
As social care providers, we receive information from a lot of different places and share it with others. This is called processing and these processes need to be recorded. Now we know what data we have, we need to consider where it comes from and where it goes.

Any data you marked as being shared externally in your IAR should be included in your Record of Processing Activities (ROPA) – you may have heard this being referred to as information mapping.

We have provided a template with examples of how this should be filled in. This template also includes possible locations you might share data with and the types of data you might share.
In general, think of what information you have which could cause upset or disruption to people or your organisation if it was accessed by the wrong person, lost, or altered unexpectedly – this is the data you should record.

All data which is physically transferred – either electronically or in hardcopy - must be added to the record. This could include: Computers, Tablets, Smart Phones, CDs, DVDs, Tapes, Answering Machines, (Digital) Photographs, Letters, Documents, Printouts, Notepads, Diaries etc.

You do not have to record information shared through face to face discussions or telephone calls but if notes are made then this information may need to form part of your records.

Exceptions for small organisations:
If you have fewer than 250 employees, you only need to record processing which happens routinely (even if that means only once every couple of years). You do not need to record one off or unexpected processing. You only need to record data processing which is likely to result in a risk to the rights and freedoms of individuals or if the data is special category. You also need to record all personal data relating to criminal convictions.

If you have 250 or more employees, you need to record all processing activities even if they only happen once or are unexpected.

In general think of what information you have which could cause upset or disruption to people or your organisation if it was accessed by the wrong person – that is the data you should record.

What to do

a) To process personal data, the processing must be necessary, i.e. if you could not perform a required activity without using the information then it is necessary. Once you know it is necessary then a legal basis for the processing must be given.

There are 6 legal bases for processing personal data under GDPR and at least one should be recorded on the ROPA (in the template these are in a drop-down list). There is guidance on each basis on the Key Definitions page. These are called Article 6 Conditions. No one condition is better than any other.

<table>
<thead>
<tr>
<th>6(1)(a) Consent</th>
<th>6(1)(b) Contract</th>
</tr>
</thead>
<tbody>
<tr>
<td>6(1)(c) Legal Obligation</td>
<td>6(1)(d) Vital Interests</td>
</tr>
<tr>
<td>6(1)(e) Public Task</td>
<td>6(1)(f) Legitimate Interest</td>
</tr>
</tbody>
</table>

b) As we know, some personal data is also considered to be special category. For most care providers, most of your special category data will be health and care data. To process special category data, you need to fulfil one of the following conditions (Article 9 conditions) as well as one of the conditions above:

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>9(2)(c) Vital interests when an individual is legally or physically unable to give consent</td>
<td>9(2)(d) Legitimate activities by a foundation, association or any other not-for-profit body</td>
</tr>
<tr>
<td>Type of processing</td>
<td>Article 6 Condition</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Sharing for direct care or administrative purposes (e.g. waiting list management) | For **NHS or LA funded** care this will be 6(1)(e) Public Task because it has been commissioned by a public body.  
For **Privately Funded** care this will be 6(1)(b) Contract  
You can also use 6(1)(c) Legal Obligation because services registered with the Care Quality Commission (CQC) are required to maintain contemporaneous records of care under the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014: Regulation 17. | 9(2)(h) the provision of health and social care                                                                 |
| For legal reasons (i.e. CQC)                          | 6(1)(c) Legal Obligation                                                                               | 9(2)(j) public interest                                                                 |
| Safeguarding                                           | 6(1)(e) Public Task                                                                                    | 9(2)(b) Employment, Social Security, Social Protection Law                             |
| Employment purposes                                    | This will depend on the type of employee data collected. In many instances this will be 6(1)(c) Legal Obligation (e.g. when providing details to HMRC – you need to be able to point to the legislation here)  
In some instances, this might also be 6(1)(f) Legitimate interests (e.g. NMDS-SC submissions) | If special category data (i.e. sick notes) are processed then the condition would be 9(2)(b) Employment, Social Security, Social Protection Law |
| Criminal records checks (DBS)                          | **Criminal records data is not covered by the GDPR as it is not classed as special category. This will instead be covered in the Data Protection Bill (which will become the Data Protection Act 2018). We will update this table with information from the Data Protection Act when it is enacted.** |                                                                                       |
A note on consent: Consent is very important in health and social care. For common law confidentiality purposes, consent (implied or explicit) is still a valid reason for sharing information. Consent is also a legal basis under GDPR, but the GDPR has stricter rules on consent which may be hard to achieve for social care providers. For the purposes of GDPR we recommend that you look for a different legal basis for processing. This does not mean you should change your current consent practices where these are used for common law or social care best practise purposes. There is extensive guidance on consent under GDPR here: https://digital.nhs.uk/information-governance-alliance/General-Data-Protection-Regulation-guidance

c) Once you have completed the legal basis for processing then complete the rest of the ROPA template – you can use your own if you prefer.

d) One of the columns asks about Data Protection Impact Assessments – we will provide separate guidance for this.

Step Three – Privacy Notices
Where you are processing personal data, you have a duty to tell people what you are doing with their data. For example, when you have a new client, you need to tell them that you might share parts of their care data with other health and care practitioners in order to care for them properly. This is called a transparency notice, privacy notice or a privacy statement. In this you need to set out in clear and easily understood language what you do with the personal data you process.

It is not necessary that each person sees the full notice, but it does need to be publicly available. For example, it might make more sense to provide a new employee with the part of the privacy notice which talks about their data and then tell them where the full notice can be found rather than provide them with a long document.

Much of the data which should be included in the privacy notice is also included in the ROPA – which is why you should complete the first two steps before putting together your privacy notice.

We have provided a draft, but this will have to be altered based on your organisation. Hopefully, once your ROPA is completed this should not be an arduous task. There is also very detailed guidance on Privacy Notices here: https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/privacy-notices-under-the-eu-general-data-protection-regulation/.

Further Information

https://digital.nhs.uk/information-governance-alliance/General-Data-Protection-Regulation-guidance - see the guidance on lawful processing. Note that this guidance is aimed at health and social care generally and focusses on public authorities.