

Section	Title	Page
1	Introduction	1-2
2	Purpose	2
3	Scope	2
4	Deciding to Share	2-3
5	Data Sharing Agreements	3-4
6	Data Protection Principles	4
7	Recording the Sharing	4
8	Fairness and Transparency	5
9	Lawful Basis for Sharing Personal Data	5
10	Security	5-6
11	Individuals Rights	6
12	Sharing Children’s Personal Data	6-7
13	Sharing in an Emergency	7
14	Implementation and Policy Management	7

~~~~~

|   |              |     |
|---|--------------|-----|
| 1 | Introduction | 1-2 |
|---|--------------|-----|

- 1.1. This Data Sharing Policy (this “Policy”) sets out the approach Polyco Healthline Limited (“Polyco Healthline”, “we”, “us”, “our”) will adopt in relation to data sharing. Polyco Healthline Limited are registered as a controller in the UK with the Information Commissioner’s Office (“ICO”), registration number Z1836501.
- 1.2. We acknowledge that there are benefits in sharing personal data, but that this practice can also give rise to risks. We will give due consideration to those risks and only share personal data in accordance with the law. The ICO has issued a Data Sharing Code of Practice and we are committed to following this.
- 1.3. This Policy has been prepared with due regard to the data protection laws applicable to us and our personal data processing activities. These data protection laws include the UK General Data Protection Regulation, the EU General Data Protection Regulation 2016/679 (where applicable) (together the “GDPR”) and the Data Protection Act 2018 (“DPA18”), collectively referred to throughout this Policy as the “Data Protection Law”.

- 1.4. This Policy should be read together with the following related documents:
- a) Polyco Healthline Data Protection Policy
  - b) Polyco Healthline Data Protection Impact Assessment Policy and Template
  - c) Polyco Healthline Legitimate Interests Assessment Template
  - d) Polyco Healthline Data Subjects' Rights Procedure

**Please note, that the definitions for any undefined terms in this Policy can be found in clause 4.1 of our Data Protection Policy and are applicable to this Policy.**

|          |         |   |
|----------|---------|---|
| <b>2</b> | Purpose | 2 |
|----------|---------|---|

2.1 The purpose of this Policy is to document our approach to the sharing of personal data.

By complying with this Policy, we will ensure that:

- All employees are clear on the issues which need to be considered and the procedures which need to be followed before any personal data is shared;
- Expected standards are met;
- Sharing of personal data will only be carried out when it is lawful, justified, necessary and proportionate to do so;
- The data protection principles and individuals' rights will be observed and adhered to; and
- The sharing will be documented.

|          |       |   |
|----------|-------|---|
| <b>3</b> | Scope | 2 |
|----------|-------|---|

3.1 This Policy applies to all our employees, workers, contractors, consultants and interns whether on full time, part time, temporary or permanent contracts.

|          |                   |     |
|----------|-------------------|-----|
| <b>4</b> | Deciding to Share | 2-3 |
|----------|-------------------|-----|

4.1 Considerations

4.1.1 Before sharing any personal data, we will consider:

- what information needs to be shared (the categories of personal data);
- if any of the personal data is particularly private or sensitive (does it include any special category data or criminal information?);
- who it will be shared with (what do we know about the third party we propose to share with?);
- for what purpose it will be shared (why do we need to share the information?);
- in what manner it will be shared (will we share it by email/secure portal etc);
- for how long the sharing will continue (is this an ongoing arrangement or a 'one-off' transfer?);

- if the sharing gives rise to any risks (include, not only privacy risks, but other risks such as risk of harm, risk of financial loss, etc);
- if the personal data is to be transferred to a third country? (If so, what safeguards are in place?);
- if the sharing is necessary or could the same outcome be achieved without the sharing;
- what will happen if we could not proceed with the sharing; and
- how will we ensure the personal data is secure.

4.2 The above list is not exhaustive and provides only an idea of the type of issues we need to consider. The most appropriate way to fully assess the position is to conduct a Data Protection Impact Assessment (“DPIA”). See below.

### 4.3 Data Protection Impact Assessments

4.3.1 A DPIA is required when the processing of personal data is likely to result in a high risk to the rights and freedoms of individuals. In order to assess the risk, the screening questions within our DPIA Template should be answered. If the result of this is that a DPIA is required, the DPIA procedure should be followed, as set out in our DPIA procedure, policy and template. An outline of the procedure is set out below:

- 1) Identify if a DPIA is needed;
- 2) Describe the processing;
- 3) Consult with stakeholders;
- 4) Assess whether the processing is necessary and proportionate;
- 5) Identify and assess whether there are any risks; and
- 6) Identify how to mitigate the risks.

### 4.4 Authorisation to Share

4.4.1 If the risks of sharing the personal data are mitigated and it is decided that the sharing will be justified, lawful, necessary and proportionate, the sharing needs to be authorised by the head of the department that is proposing to share, in consultation with the IT Manager.

|          |                                |            |
|----------|--------------------------------|------------|
| <b>5</b> | <b>Data Sharing Agreements</b> | <b>3-4</b> |
|----------|--------------------------------|------------|

5.1 Once it has been decided that the sharing will proceed, steps should be taken to ensure that the obligations and responsibilities of each party are recorded in writing. This will help to ensure that we are all clear on how the arrangement will work and what the expectations are.

5.2 The most appropriate way to document the arrangement is to ensure that we enter into a Data Sharing Agreement. This Agreement should include:

- 1) Details of the data to be shared (including any specific arrangements for sharing special category data or criminal information);
- 2) The purpose of sharing;

- 3) The responsibilities and obligations of each party;
- 4) The lawful basis for sharing, together with the relevant condition(s), where necessary. (See below under 'Lawful Basis for Sharing Personal Data');
- 5) Agreed retention periods;
- 6) Security measures; and
- 7) How you will address data subject rights requests.

|          |                            |   |
|----------|----------------------------|---|
| <b>6</b> | Data Protection Principles | 4 |
|----------|----------------------------|---|

- 6.1 When sharing any personal data, we will ensure that we will adhere to the data protection principles as set out in the Data Protection Law. We will ensure that the personal data will be:
- Processed lawfully, fairly and in a transparent manner;
  - Collected for specified, explicit and legitimate purposes;
  - Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
  - Accurate and, where necessary, kept up to date;
  - Kept for no longer than is necessary; and
  - Processed in a manner that ensures appropriate security of the personal data.

|          |                       |   |
|----------|-----------------------|---|
| <b>7</b> | Recording the Sharing | 4 |
|----------|-----------------------|---|

- 7.1 The Data Protection Law requires us to document our processing activities, including any sharing of personal data. We will keep details of the data sharing arrangements we enter into, in a Data Sharing Register.
- 7.2 The Data Sharing Register will contain the following information:
- Details of the decision to share including the justification for sharing;
  - Details of what information was shared;
  - The purpose of the sharing;
  - With whom the personal data was shared;
  - The lawful basis;
  - Whether consent was obtained for the sharing; and
  - Details of the Data Sharing Agreement entered into.
- 7.3 In addition to the above, in order to satisfy the 'Accountability' principle under the Data Protection Law, we will retain the following documentation:
- A copy of any DPIAs we carry out in relation to the sharing;
  - Data Sharing Agreements;
  - The Data Sharing Register; and
  - Privacy Notices that refer to the sharing (where necessary).

|          |                           |   |
|----------|---------------------------|---|
| <b>8</b> | Fairness and Transparency | 5 |
|----------|---------------------------|---|

- 8.1 We have a legal obligation to ensure that, if we share personal data, we do so in a fair and transparent manner, in accordance with the first GDPR data protection principle. In order to meet this requirement, we will be open with individuals and tell them who we are sharing their personal data with by setting this out in our privacy notices.
- 8.2 If any occasions arise in which we do not wish to tell the individual who we are sharing their personal data with, we will take advice from the IT Manager. There are exemptions under the Data Protection Law that could be relied upon, depending on the circumstances, but each case must be assessed individually.

|          |                                        |   |
|----------|----------------------------------------|---|
| <b>9</b> | Lawful Basis for Sharing Personal Data | 5 |
|----------|----------------------------------------|---|

- 9.1 Under Article 6 GDPR, we need to identify a lawful basis for all the processing activities we carry out, including sharing. There are six lawful bases:
  - Consent;
  - Contract;
  - Legal obligation;
  - Vital interests;
  - Carrying out a task in the public interest; and
  - Legitimate interests.
- 9.2 If the personal data to be shared is classed as special category data, a condition under Article 9 GDPR will also need to be satisfied and, in some cases, a condition under the DPA18 will also need to be identified.
- 9.3 If the personal data to be shared is information relating to criminal information, Article 10 GDPR needs to be observed and a condition under the DPA18 may also need to be identified.
- 9.4 Once we have identified our lawful basis for the sharing, together with the relevant condition(s) (where necessary), we will record this in our Data Sharing Agreement and Data Sharing Register. If consent is to be relied upon, we must retain evidence of the consent. If legitimate interests is to be relied upon, we will conduct a Legitimate Interests Assessment (“LIA”) and retain this as evidence. (See our LIA Template).

|           |          |     |
|-----------|----------|-----|
| <b>10</b> | Security | 5-6 |
|-----------|----------|-----|

- 10.1 Under the Data Protection Law, we have an obligation to implement appropriate technical and organisational measures to safeguard personal data. When sharing personal data, we will ensure that we adhere to our usual security procedures.

10.2 We will take reasonable steps to ensure that the personal data we share will continue to be protected once we have released it. Our Data Sharing Agreement will set out details of the security measures required of the organisation we are sharing the personal data with.

|           |                           |          |
|-----------|---------------------------|----------|
| <b>11</b> | <b>Individuals Rights</b> | <b>6</b> |
|-----------|---------------------------|----------|

11.1 Individuals have rights under the Data Protection Law. These are explained in our Data Subjects' Rights Request Policy, together with the procedures to follow when an individual wishes to exercise their rights. The rights are:

- The right of access to their personal data;
- The right to be informed that personal data is being processed;
- The right to have personal data rectified, erased or restricted;
- The right to object to processing;
- The right to data portability; and
- The right not to be subject to a decision based solely on automated processing.

11.2 In a data sharing arrangement, individuals could submit a request to exercise their rights to us or to the party we have shared their personal data with. Our Data Sharing Agreement will set out how we will address this situation to ensure that we respond appropriately and within the permitted time scales.

|           |                                         |            |
|-----------|-----------------------------------------|------------|
| <b>12</b> | <b>Sharing Children's Personal Data</b> | <b>6-7</b> |
|-----------|-----------------------------------------|------------|

12.1 If we are considering sharing the personal data of children, we must be very careful. Children are vulnerable and are not as aware as adults of the risks that may be involved in sharing their personal data. Anything we do with children's personal data must be in the child's best interests.

12.2 Before sharing children's personal data we will:

- Conduct a Data Protection Impact Assessment;
- Carry out due diligence checks on the company we are proposing to share the personal data with and if we discover that they are planning to do something with the personal data that could be detrimental or unfair to the children, we should not proceed with the sharing;
- Ensure privacy notices provided to the children are clear and easy for a child to understand (using diagrams, graphics or cartoons, where necessary); and
- If we are relying on consent or contract as the lawful basis, we need to ensure that the child is competent to provide consent or enter into a contract, in that they are of sufficient age and maturity to fully understand what they are consenting / contracting to.

12.3 If any of the controllers involved in the sharing of children's personal data are a provider of online services that are likely to be used by children, the Age-Appropriate Design Code will need to be complied with, to ensure the obligations under the Data Protection Law, to protect children's data online, are met.

|    |                         |   |
|----|-------------------------|---|
| 13 | Sharing in an Emergency | 7 |
|----|-------------------------|---|

13.1 This Policy focusses on situations where we can plan who we share personal data with and will have time to carefully consider all the issues. However, in an emergency we will not have time to do this, but we should proceed with sharing in an emergency if it is necessary to:

- a) Prevent serious physical harm or loss of life;
- b) Protect public health or national security; and
- c) Safeguard vulnerable adults or children.

|    |                                      |   |
|----|--------------------------------------|---|
| 14 | Implementation and Policy Management | 7 |
|----|--------------------------------------|---|

14.1 This procedure shall be deemed effective as of 01.02.2022. No part of this procedure shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy will be reviewed by the GDPR Committee annually and following any personal data breach.

**Signature:**



**Place of Issue:** Bourne, PE10 0DN, UK

**Name:** Jack Prichard

**Date:** 11th June 2024

**Position:** Chief Executive Officer