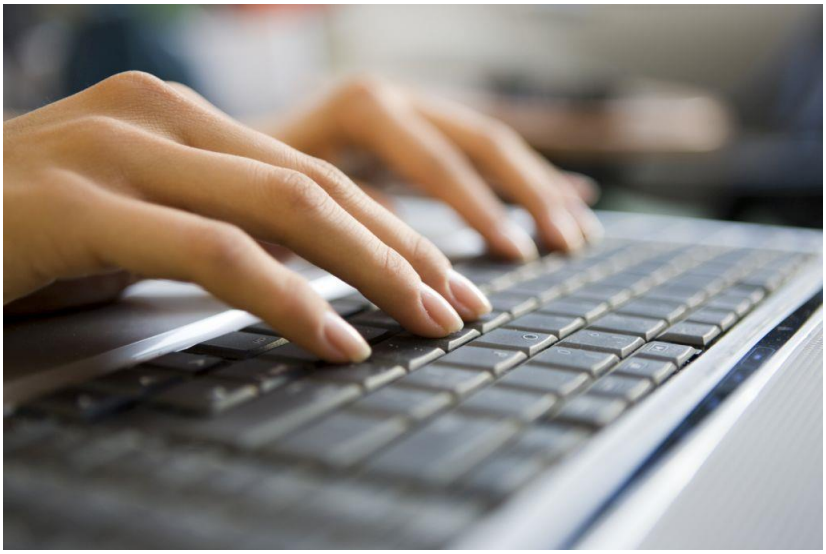
SOUTH WEST INFORMATION SHARING

South West Information Sharing (SWIS)



Signatory Guide

Contents

Overview

Welcome to South West Information Sharing (SWIS) partnership and thank you for registering as a Signatory. The 'SWIS' model is designed to be a secure and efficient mechanism for the multi-agency sharing of personal and sensitive data that is compliant to the EU General Data Protection Regulations (GDPR) and the UK Data Protection Act 2018 for organisations across the South West.

The SWIS consists of a standardised Data Sharing Agreement that can be adopted by the Public, Private and Voluntary sectors to assist with the regular sharing of data. This standardised sharing agreement will require signatories to agree to a 'Tier 1' contract that sets out the legal requirements and expectations of data sharing in accordance to data protection law.

The 'Tier 2' component of the document can be tailored to the specific needs and requirements of individual data sharing partnerships. The Partnership aims to create a more joined up approach to data sharing, making business processes more succinct, efficient and legally compliant.

The SWIS is required as a result of the implantation of the GDPR and the UK Data Protection Act in May 2018 which has placed greater accountability on Data Controllers and Processors over the ways in which personal data is managed, including the sharing of this information. Organisations and businesses collect process and disclose personal and sensitive data of their customers with third party processors for a variety of reasons such as to facilitate joined up decision making, and in the interests of the public or their clientele. This must be carried out in accordance with data protection legislation, hence the need for a unified data sharing template.

The Information Commissioners Office (ICO) state that for data sharing to be lawful, it must:

- ✓ Be proportionate and necessary for its intended use
- ✓ Be up to date and accurate
- ✓ Be provided with the necessary consent and privacy information
- ✓ Be well documented
- ✓ Be secure and have protection measures in place

By registering your organisation with the 'SWIS' partnership, you are accepting the terms of the agreement and confirm that your organisation will liaise with other signatories accordingly, and that you have the necessary due diligence procedures in place to process and share personal data. You can withdraw from the partnership at any time visiting the 'Opt Out' section of the SWIS website.

Lawful Basis for Data Sharing

Under data protection law, there must be a lawful basis for the disclosure of personal or sensitive data. When looking to disclose or share personal data with any other third-party processor, you must be sure which of the lawful basis applies to your need to share data, and you must be able to justify this decision. The ICO defines the different lawful basis' as:

- ✓ **Legitimate Interests** – the data sharing is genuinely in the interests of both or either the data controller or the data subject.
- ✓ **Consent** – The data subject has explicitly granted their consent to the data sharing
- ✓ **Contractual** – the data controller has a legal contract with the data subject(s) enabling them to share data to satisfy this contract
- ✓ **Legal** – The data is required for legal purposes i.e. if requested by the police, to satisfy a law or if required for judicial purposes
- ✓ **Public Interest** – If the data is needed in the public interest. Most relevant to local authorities and the public sector

- ✓ **Vital Interest** – If the data is required in the vital interests of the data subject. I.e. may be used by the ambulance service or NHS in the interests of the individual's safety and wellbeing.

If you are relying on Consent as your lawful basis, you must ensure that the Data Subject has freely and unambiguously opted-in to the sharing of their data. This consent mechanism must then be documented and stored securely. It is important to remember that under the 'GDPR', data subjects also have the right to withdraw their consent at any point, and it must be as easy to withdraw consent as it is to give it, therefore highlighting the importance of accurate record keeping.

More information and advice on this can be found on the ICO website: https://ico.org.uk/

The Risks of Data Sharing & Privacy Impact Assessments

The sharing of personal or sensitive data carries considerable risk. It is there a requirement of 'SWIS' membership that Signatories recognise this risk and have suitable organisational and technical measures in place to protect the data they are disclosing and processing.

Data can be shared and disclosed both in hard copy or digitally, therefore considerations must be made by the data controller as to the most appropriate method of sharing the data and to weigh up the associated risks of each method – it is likely there will be pro's and con's to each. It is therefore best practise to conduct a thorough Data Privacy Impact Assessment (DPIA) before entering into a data sharing partnership. The 'DPIA' will encourage you to think about:

- ✓ The most appropriate method of data sharing (physical or digital)
- ✓ To assess the necessity of the data sharing
- ✓ To assess what resources and protection measures are required
- ✓ To identify the key risks
- ✓ To develop an action plan to mitigate the risks

More information and DPIA templates can be found at the ICO website: https://ico.org.uk/. Any significant risks identified in a DPIA should be declared in Tier 2 of the Data Sharing

Agreement template. There are 'quick fix' steps that can be taken by all organisations to reduce the risk to data including:

- ✓ Ensuring you have secure email encryption if sharing data digitally and take care when using the 'autofill' function when entering email addresses. Use the 'BCC' function when emailing various people to protect their privacy
- ✓ Change network access passwords regularly
- ✓ If personal data is sent via post, send using secure/tracked service
- ✓ Always operate a clear desk policy in offices
- ✓ Take care when working remotely and limit carrying around personal data in hard copy
- ✓ Take care when removing paperwork/letters from printers – check you haven't taken someone else's data!

Tier 1 & Tier 2 Data Sharing Agreement

The SWIS Data Sharing template has been developed to facilitate improved and secure data sharing provisions amongst partner organisations that is compliant to the updated data protection legislation. Tier 2 Agreements must be signed off by the Data Protection Officer of each organisation/data controller and be saved securely for audit purposes.

- **Tier 1 –** This is the overarching strategic document that all signatories must comply with. It covers off the legalities around the data sharing and the data protection laws. This is a standardised contract that can be applied to all sectors and cannot be amended or changed.

- **Tier 2 –** This is the part of the document that can be edited to suit the specific needs and requirements of individual data sharing partnerships. This should detail:

    - ✓ The overall purpose and legal basis for the data sharing
    - ✓ The information that will be shared
    - ✓ The method of sharing the data
    - ✓ Security measures in place to safeguard data
    - ✓ Retention periods
    - ✓ Procedures to action data breaches and data subject rights

Tier 2 Agreement must be established with each signatory that you intend to work with as soon as you have registered with the partnership under the Tier 1 agreement. Tier 2

agreements should be periodically reviewed and updated if necessary, to ensure the document remains fit for purpose and relevant.

Data Subject Rights

The SWIS charter recognises the individual rights that the 'GDPR' empowers Data Subjects with and this is reflected in the Tier 1 Agreement. All signatories must be aware of these rights and have appropriate procedures in place to action these rights should they ever need to. These rights are:

- ✓ **The right to be informed** – (the provision of privacy notices)
- ✓ **The right of access** – (Subject Access Requests)
- ✓ **The right to data portability** – (data transferred from one controller to another)
- ✓ **The right to rectification** – (correcting inaccurate data)
- ✓ **The right to erasure** – (deleting data entirely from systems/databases)
- ✓ **The right to restrict processing** – (restricting the processing of certain data)
- ✓ **The right to object** – (objecting to the processing of certain data)
- ✓ **Rights in relation to profiling** – (right to grant/withdraw explicit consent)

The Data Protection Act 2018 and the 'GDPR' dictates that all of the above rights must be actioned within one month, unless in exceptional circumstances and can be received in any

format (written, verbal or digitally). The law also dictates that data controller's can no longer impose administration fees on processing any of the above rights unless in exceptional circumstances. Signatories should detail in the Tier 2 Agreement what processes they have in place to deal with the above rights efficiently.

More information on data subject rights can be found on the ICO website: https://ico.org.uk/.

Categories of Data and Data Protection Principles

The Data Protection Act 2018 consists of 7 key principles that should be reflected in the Tier 2 Data Sharing Agreements, and that underpin the 'SWIS' Charter. These 7 principles are:

1. Data is processed fairly, lawfully and with complete transparency
2. Data is collected for legitimate, explicit and specified purposes
3. Data is adequate, relevant and limited to what is necessary
4. Data is kept accurate and up to date
5. Data is kept for no longer than is necessary with clear retention periods
6. Data is processed securely to minimise risk of data loss/breach
7. Data Controllers can demonstrate the above data governance

The above principles are especially significant when processing 'sensitive' or 'special category' data. Under data protection law, there is a differentiation between data that is considered 'personal' and 'sensitive'. Special Category/Sensitive data includes:

- ✓ Health and Medical Data
- ✓ Criminal Conviction Data
- ✓ Religion

- ✓ Political Views
- ✓ Trade Union Membership
- ✓ Sexuality
- ✓ Race/Ethnic Origin
- ✓ Biometric Data