derbyshire partnership forum

Information Sharing Protocol

June 2018

Abstract

Guidance and template for Information Sharing Agreements for organisations within the Derbyshire Partnership Forum

V5.1

Version	5.1
Date	30 November 2018
Author	Mel Turvey, Policy and Research, Commissioning, Communities and Policy, Derbyshire County Council
Document Owner	Derbyshire Partnership Forum
Approving Committee	Derbyshire County Council Information Governance Group, Derbyshire Information Governance Network, Derbyshire Partnership Forum
Review Date	June 2020
Document Classification	**PUBLIC**

Change History

Version	Date	Description of change
4.0	April 2016	Agreed by Information Governance Group (IGG), Derbyshire County Council, Derby City Council, Derbyshire Community Health Services NHS Foundation Trust and Arden and GEM CSU
4.1	January 2018	GDPR updates added by Mel Turvey, Derbyshire County Council
4.2	April 2018	Updates to ISA template (Appendix 2) – Mel Turvey & Janet Gardom
4.3	April 2018	Simplify and reduce document
4.4	May 2018	Reorganise structure of the document and update consent (not finished) – Mel Turvey
4.5	25 May 2018	Updates from Data Protection Act 2018 and Template – Mel Turvey & Janet Gardom
4.6	30 May 2018	Minor changes to wording and removal of Direct Care Model of consent, Comments back from IGG – Mel Turvey, Neil Brailsford, Janet Gardom
5.0	1 June 2018	Consent and finalisation of document – Mel Turvey
5.0	11 June 2018	Agreed by Information Governance Group (IGG), Derbyshire County Council
5.1	30 November 2018	Feedback from Derbyshire Partnership Forum members and Derbyshire Information Governance Network (DIGN) group Updates to pages sections 6, 11.2 and Appendix 2, Template, Appendix 3 – Legal Framework, and Appendix 8 Flowchart

Contents

A glossary for terms used throughout this document is available in Appendix 1

1. Purpose of the Information Sharing Protocol

The Derbyshire Partnership Forum is committed to working together, putting the individual at its heart for the improved planning and delivery of Derbyshire's public services, safeguarding and to promote the welfare of children and adults.

To work well in partnership, we need to share information, including sensitive personal data, between individuals, professions and organisations – including public, private and voluntary sectors. Effective and structured sharing of information between partners has the ability to inform care and planning, allows us to understand trends and patterns of activity, to respond to emergencies appropriately, and to support the lives and safety of individuals, families and communities. At a time when the gathering and storing of information continues to increase, we have a moral and statutory responsibility. We need to be able to share information carefully and responsibly and to assure service users, patients, carers, practitioners, providers, the public and partners that information held about them or from their organisation is shared securely and appropriately, whilst also respecting an individual's right to privacy and confidentiality. Effective use of information will support us in achieving all the ambitions and aspirations we have for those living in Derby and Derbyshire.

The purpose of this overarching Protocol is to set out a framework for partner organisations and their staff to manage, process and share personal and sensitive personal information on a lawful, fair and transparent basis with the purpose of enabling them to meet both their statutory obligations and the needs and expectations of the people they serve.

All organisations should play a role in supporting the sharing of information between and within organisations and address any barriers to information sharing to ensure that a culture of appropriate information sharing is developed and supported.

This document sets out the overarching principles and commitments that will underpin the secure and confidential sharing of information between organisations involved in delivering services to people living and working within Derby and Derbyshire and contains a template to create an Information Sharing Agreement (ISA) (see Appendix 2) between yourselves and other organisations within the Partnership.

Specifically, this Protocol aims to:

- Set out generally what information will be shared
- Set out the general principles of information sharing
- Identify the lawful basis for sharing information
- Define the common purposes for holding and sharing data
- Promotes a standard approach to the development of Information Sharing Agreements
- Set out how information will be stored
- Identify the partner organisations who are signatories to this Protocol

This Protocol applies to chief officers, elected members, executive directors, non-executive directors, trustees and all employees including volunteers and agency staff of the organisation and partner organisations who are signatories.

The Protocol also applies to any organisation or agency which has been commissioned to deliver services on behalf of any organisation party to this Protocol where permission has been given to the third party organisation to disclose information by consent of the Data Controller.

The Protocol is intended to complement any existing professional Codes of Practice that apply to any relevant profession working within any organisation including the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA), but does not cover an individual organisations compliance to the GDPR or DPA and does not constitute legal advice. See Appendix 3 for a list of relevant legislation that may affect your ability to share information.

2. What is data sharing?

By 'data sharing' we mean the disclosure of data or information from one or more organisations to a third party organisation or organisations, or the sharing of data between different parts of an organisation. Data sharing can take the form of:

- a reciprocal exchange of data
- one or more organisations providing data to a third party or parties
- several organisations pooling data and making it available to each other
- several organisations pooling data and making it available to a third party or parties
- exceptional, one-off disclosures of data in unexpected or emergency situations
- different parts of the same organisation making data available to each other (this type of data sharing could be subject to internal ISAs as defined by your own organisation)

There are two main types of data sharing:

2.1 Systematic data sharing

This will generally involve routine sharing of data sets between organisations for an agreed purpose. It could also involve a group of organisations making an arrangement to 'pool' their data for specific purposes.

2.2 Exceptional data sharing

The majority of data sharing takes place in a pre-planned and routine way and this Protocol sets out the principles for effective information sharing and the establishment of Information Sharing Agreements. However, organisations may also decide, or be asked, to share data in situations which are not covered by any routine agreement i.e. one-off decision to share data for a range of purposes. In some cases this may involve a decision about sharing being made in conditions of real urgency, for example in an emergency situation if a patient lacks the capacity to give consent.

Different approaches apply to these two types of data sharing and this Protocol and resulting sharing agreements need to reflect this. Some of the good practice recommendations that are relevant to systematic, routine data sharing are not applicable to one-off decisions about sharing. In either case however, the sharing of personal data must comply with the requirements of the legislation.

3. Who can we share data with?

Data can be shared within organisations, with partner organisations either as a **'Data Controller'** or as a **'Data Processor'** and with third parties as a 'Sub Data Processor'.

3.1 Sharing with a 'data controller'

The Information Commissioners Office (ICO) define a data controller as "a body who determines the purposes and means of processing personal data." The majority of instances where data is to be shared under this Protocol and any ISAs are predominantly about sharing personal data between data controllers.

Data controllers, under the GDPR guidelines now have the added responsibility to ensure that all contracts and ISAs comply with the GDPR.

For more information please see the ICO website https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf

3.2 Sharing with a 'data processor'

Where a data controller shares data with another party that is responsible for the processing of personal data on its behalf, the GDPR, DPA and ICO identifies these organisations as 'data processors'.

If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach. See Appendix 4 for more information on the GDPR.

A data controller using a data processor must ensure, in a written contract, that:

- the processor only acts on instructions from the data controller; and
- it has security in place that is equivalent to that imposed on the data controller by the sixth data protection principle, see DPA Act Principles Appendix 5.

Information sharing is not solely limited to Partners who are party to this Protocol. It may be that there is a need to share information across departments or with national partners or other organisations not in the Derbyshire Partnership. The GDPR and the DPA should not hinder the sharing of information but allow you to securely and lawfully process and manage information flows.

3.2.1 Sharing within organisations

Data sharing and the data protection principles also apply to the sharing of information between the different departments of an organisation such as local authority or financial services company. An approach and willingness to share information across departments should be encouraged to support the needs of the wider organisation whilst adhering to the principles and requirements set out within this Protocol. Please see your own organisations procedures for guidance.

3.2.2 Sharing with organisations who are not signatories to this protocol

Any organisation who is not party to this overarching Protocol, but who wishes to share information may do so, providing that there is an existing Information Sharing Agreement or contract in place with the third party, that they agree to comply with the terms of this overarching Protocol and have adequate technical and non-technical security arrangements in place, for example compliance with the Information Governance Toolkit. Or, for example it may be required for your organisation to adhere to another Information Sharing Protocol/Agreement as set out by another Data Controller such as Public Health England, this would need to be reviewed and agreed by your own organisation.

Once a need to share information between organisations has been identified and the Information Sharing Agreement has been agreed by all Parties then all of the organisations are responsible for providing a culture of support to ensure that good practice in information sharing is promoted and supported.

The following range of purposes are agreed as justifiable for the transfer of personal confidential information between the partner agencies as defined within the remit of this Protocol from which organisations aim to establish:

- A culture that supports information sharing between and within organisations including proactive mechanisms for identifying and resolving potential issues and opportunities for reflective practice.
- A systematic approach to explain to service users when the service is first accessed, how and why information may be shared.
- Clear systems, standards and procedures for ensuring the security of information and for information sharing.
- Infrastructure and systems to support secure information sharing, for example, access to secure email or online information systems.
- Effective supervision and support in developing practitioners and managers professionals' judgement in making these decisions.
- Mechanisms for monitoring and auditing information sharing practice.
- Designated source of impartial advice and support on information sharing issues, and for resolution of any difference of opinion about information sharing.
- There is an established information sharing governance framework so that staff are clear about the organisations position on information sharing.
- Information sharing governance framework must always recognise the importance of professional judgement in information sharing at the front line and should focus on how to improve practice in information sharing within and between agencies.

4. What data can we share?

The Protocol applies to the following types of data:

4.1 Personal data

The GDPR and DPA (see Appendices 4 and 5) identifies two types of data Personal and Sensitive personal data (or special category data), both relate to living people (Data Subjects). However the Caldicott Information Guardian Review identified a third classification of Personal Confidential Data (PCD), which relates to both living and deceased individuals (see Appendix 6).

4.1.1 Personal data means data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of the data controller. Such data could include the data subjects name, address, bank details or IP address. Whilst a name on its own may not be enough to identify an individual when it is linked to other information then it will become identifiable and therefore 'personal data'.

4.1.2 Sensitive personal data or special category data Certain types of personal information have been classified as sensitive data, the GDPR and DPA (which relates to

living individuals only) provides that additional conditions must be met for that information to be used and disclosed lawfully. The term 'sensitive' data refers to information that provides details of:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- Trade Union membership
- physical or mental health
- sexual life or orientation
- processing of generic biometric data for the purpose of uniquely identifying a natural person
- or commission or alleged commission of an offence, criminal proceedings or sentence.

4.1.3 Personal confidential data (PCD) describes personal information about identified or identifiable individuals which should be kept private or secret and refers to any information held either as manual and/or electronic records, or records held by means of audio and /or visual technology, about a living or deceased individual who can be personally identified from that information. Examples of identifiable data are Name, address, postcode, date of birth, NHS number.

Some data sharing does not involve personal data, for example where only statistical data that cannot identify anyone is being shared. Neither the GDPR, DPA nor this Protocol, apply to that type of sharing provided that an individual cannot be identified (see par 4.2 and 4.3 below).

4.2 Anonymised and Pseudonymised information

Information that falls into this category is data about people that has been aggregated, tabulated or has had unique identifier replaced or removed in ways that make it impossible to identify the details of individuals. This can be shared without the consent of the individuals involved and the processing is outside the provisions of the GDPR and DPA. However, care should be taken to ensure that it should not be possible to identify individuals either directly or in summation. This can happen when anonymised information is combined with other data from different organisations, where the aggregated results produce small numbers in a sample, or where traceable reference numbers are used. Further guidance on anonymised information and requirements can be found in the Information Commissioners Office 'Code of Practice on Anonymisation'. https://ico.org.uk/media/1061/anonymisation-code.pdf

4.3 Non-personal information

Information that does not relate to people; e.g. information about organisations, natural resources and projects, or information about people that has been aggregated to a level that is not about individuals.

There is a general presumption and expectation that anonymised and non-personal information will be shared, unless there are exceptional reasons for this. These may include:

- commercial confidentiality

- where disclosure may forfeit the organisations duty to ensure safe and efficient conduct of organisational operations
- policy formulation (where a policy is under development and circulation would prejudice its development)
- protect other legal and contractual obligations, and
- where information is marked protectively (for more information refer to your organisations standards for information classifications).

5. When can we share data?

Each of the signatory agencies, their staff and representatives, agree to share information between them, to the extent that is fair and lawful. Information will only be shared for a specific lawful purpose or where appropriate consent has been obtained.

There are six lawful bases to processing personal data and at least one of these must apply whenever you process personal data:

1. Consent: the individual has given clear consent for you to process their personal data for a specific purpose. See Appendix 7 for further guidance on consent.
2. Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
3. Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations), an example would be if the Council needs to use the data for the safeguarding of adults or children.

   For more information in a safeguarding setting also see Safeguarding Seven golden rules for information sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers, HM Government, March 2015 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/419628/Information_sharing_advice_safeguarding_practitioners.pdf

4. Vital interests: the processing is necessary to protect someone's life.
5. Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
6. Legitimate interests: the processing is necessary for your 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. (This cannot apply if you are a public authority processing data to perform your official tasks.)

When is processing 'necessary'?

Many of the lawful bases for processing data depend on the processing being "necessary". This does not mean that processing always has to be essential. However, it must be a targeted and proportionate way of achieving the purpose. The lawful basis will not apply if you can reasonably achieve the purpose by some other less intrusive means.

It is not enough to argue that processing is necessary because you have chosen to operate your business in a particular way. The question is whether the processing is a necessary for the stated purpose, not whether it is a necessary part of your chosen method of pursuing that purpose.

How do we decide which lawful basis applies?

This depends on your specific purposes and the context of the processing. You should consider which lawful basis best fits the circumstances. You might consider that more than one basis applies, in which case you should identify and document all of them from the start.

You may need to consider a variety of factors, including:

- What is your purpose – what are you trying to achieve?
- Can you reasonably achieve it in a different way?
- Do you have a choice over whether or not to process the data?

Several of the lawful bases relate to a particular specified purpose – a legal obligation, a contract with the individual, protecting someone's vital interests, or performing your public tasks. If you are processing for these purposes then the appropriate lawful basis may well be obvious, so it is helpful to consider these first.

If you are a public authority and can demonstrate that the processing is to perform your tasks as set down in UK law, then you are able to use the public task basis. If not, you may still be able to consider consent or legitimate interests in some cases, depending on the nature of the processing and your relationship with the individual. There is no absolute ban on public authorities using consent or legitimate interests as their lawful basis, but the GDPR does restrict public authorities' use of these two bases.

See ICO GDPR for further information on lawful basis: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

6. Information Sharing Principles

This Protocol recognises that sharing of information should be done fairly and lawfully, be properly controlled and should strike a balance between the specific rights of individuals and the public interest. The following are the principles to be applied whenever personal, sensitive personal, special category or confidential information is shared or exchanged. The organisations signed up to this Protocol are fully committed to ensuring that these principles are adhered to at all times.

The principles established by this Protocol are:

- Information about individuals will only be shared when and where it is needed
- Information will be shared in accordance with statutory duties, underpinned by specific protocols and information sharing agreements where appropriate
- Information that is provided in confidence will be treated as confidential
- Information will only be used for the purposes for which it was collected and shared
- Individuals will be properly informed about the way their personal information is used and shared and told if it changes
- Consent to share personal information will be sought wherever appropriate
- Considerations of confidentiality and privacy will not automatically cease on death
- The information rights of individuals will be respected and observed
- Organisations collecting personal information will publish service-specific privacy statements and all sharing agreements.

To achieve these principles, Partner organisations agree to:

- Share information with each other where it is lawful and when they are required to do so, for more information please see the flowchart of key questions to information sharing in Appendix 8
- Adhere to the legal framework governing information sharing, see Appendix 3
- Conduct a Privacy Impact Assessment (PIA) (also known as a Data Protection Impact Assessment (DPIA)) on all new or significantly changed ISAs, please refer to your own organisations procedures to complete this
- Comply with the requirements of the DPA 2018, in particular with the six Data Protection Principles, see Appendix 5 and to register with the Information Commissioner's Office (ICO), if the organisation processes personal information (unless exempt)
- Share information in accordance to all the 7 Caldicott principles, see Appendix 6
- Inform individuals when and how information is recorded about them and how their information may be used i.e. use of privacy notices
- Ensure that adequate technical and non-technical security measures are applied to the personal data they hold and transfer
- Develop local Information Sharing Agreements Appendix 2 that govern the way transactions are undertaken between partner organisations and with other organisations that are not parties to this Protocol
- Promote staff awareness of the Protocol and any relevant Information Sharing Agreements and ensure that staff have had the appropriate level of training in information security and confidentiality
- Promote public awareness of the need for information sharing through the use of appropriate communications media
- Ensure appropriate external accreditations are achieved such as level 2 of the Data Security and Protection Toolkit, Public Services Network (PSN) compliance and/or ISO27001 (these would be dependent on your setting and data to be shared)
- Health and social care organisations share information and ensure individuals confidentiality by embedding the 5 rules into organisational systems and processes as set out by the Health and Social Care Information Centre Data Sharing Code of Practice 2013; http://www.hscic.gov.uk/confguideorg
- Include any further legislation which may be relevant to sharing information for your specific requirements such as the Health and Social Care (Safety and Quality) Act 2015, Children and Social Work Act 2017 which may not already be listed in the legal framework listed in Appendix 3.

7. Commitments in support of the Protocol

Signatories to this Protocol are committed to the implementation of an appropriate level of Information Governance throughout their organisation, in accordance with recognised national standards. They will:

- Adhere to the principles and commitments of this Protocol whenever exchanging personal information, whether with a co-signatory or other agency/organisation
- Share statistical and anonymised/pseudonymised data wherever possible, eliminating the use of personal information except where reasonably necessary

- Ensure that all staff (including temporary employees, contractors and volunteers) are aware of and comply with their responsibilities arising from both the Protocol and relevant legislation, and receive adequate training in order to do so
- Implement their own policies on confidentiality, data protection, information security, records management and information quality, which are appropriate to their organisation and comply with recognised codes of practice.

Signatories to this Protocol will also establish efficient and effective procedures for:

- Obtaining, informed consent to collect, share and process personal information wherever reasonably practicable
- Informing individuals what information is collected and shared about them
- Sharing of personal information identified as part of a detailed agreement
- Addressing complaints arising from the misuse or inappropriate disclosure of personal information arising from information sharing decisions
- Enabling access to records of individuals by those individuals on request
- Amending records where they have been shown to be inaccurate and informing partners where these are shared
- Review and destroy information in accordance with good records management practice and organisational policy
- Sharing information without consent when necessary, recording the reasons for that disclosure (including legal basis) and the person responsible for making the decision
- Making information-sharing an obligation on staff and allocating senior staff responsibility for making complex disclosure decisions
- Ensuring that personal information is protected at all times, through the use of appropriate protective marking, security and handling measures
- Develop and work to detailed, specific information sharing agreements that support identified purposes
- Ensure that future developments in technology reflect the requirements of the GDPR, DPA 2018 and this Protocol and any that any information sharing is secure and can comply with the GDPR and DPA
- Issues, incidents and complaints resulting from failures in the specific agreements will be fed into the review processes for the individual Agreements
- Share information free of charge unless special charging arrangements have been agreed
- Seek legal advice where appropriate
- Ensure their registration as Data Controllers under the DPA 2018 is adequate for the purposes for which they may need to process and share information with one another
- Support the principles of equality and diversity within the community and ensure that whenever information is provided to the public it will be supplied in appropriate formats and languages as appropriate.

8. Implementation, Monitoring and Review

The Protocol is owned by all of its signatories. The intention has been to develop an over-arching code of behaviour for all information-sharing applications. This will be supplemented by Information Sharing Agreements for specific purposes which will adopt the principles and

commitments in the Protocol as their base line and identify any additional service specific requirements.

The Protocol will be reviewed every two years and will be updated to account for any changes in legislation and developments in national guidance. Issues arising from breaches of the Protocol, changes in legislation, or recommendations arising from review may result in an earlier review.

Each partner organisation will be individually responsible for monitoring and reviewing the implementation of the Protocol and publishing any individual Information Sharing Agreements they may have.

Any of the signatories can request an extraordinary review at any time when a joint discussion or decision is necessary to tackle local service developments.

Work to develop individual Information Sharing Agreements will be the responsibility of the organisations wishing to share information as will the review of existing ISAs on updates to the Protocol, ISA Template (see Appendix 2) and changes to relevant legislation.

9. Personal data breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data. All agencies who are party to this Protocol will have in place appropriate measures to investigate and deal with personal data breaches. Personal data breaches can include:

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

In the event that personal information shared under this Protocol is or may have been compromised, whether accidental or intentional, the organisation making the discovery will, without delay:

- Inform the organisation who provided the data (Data Controller) of the details
- Take steps to investigate the cause
- Take disciplinary action against the person(s) responsible, if appropriate

- Take appropriate steps to avoid a repetition
- Take appropriate steps, where possible, to mitigate any impacts.

On being notified of a breach, the Data Controller along with the organisation responsible for the breach, and others as appropriate, will assess the potential risks and implications for the individual(s) whose information has been compromised, and if necessary will:

- Notify the individual(s) concerned
- Advise the individual(s) of their rights
- Provide the individual(s) with appropriate support
- Keep a record of any personal data breaches.

Where a breach is identified as serious, it will have to be reported to the Information Commissioner's Office (ICO) **within 72 hours** of becoming aware of the breach so notification to the Data Controller as soon as possible is advisable.

10. Complaints

Partner organisations must have in place procedures to address complaints relating to the inappropriate disclosure of information. The partner organisations agree to cooperate in any complaint investigation where they have information that is relevant to the investigation. Partners must also ensure that their complaints procedures and the contact details of the Data Protection Officer (DPO) are well publicised.

If the complaint affects more than one partner organisation it should be brought to the attention of the appropriate complaints officers/DPOs who should liaise to investigate the complaint.

11. Organisational and individual responsibilities

Disclosure of personal confidential information without consent must be justifiable on legal/statutory grounds, or meet the criterion for claiming an exemption under the DPA 2018. Without such justification, both the organisation and the member of staff expose themselves to the risk of prosecution and liability to a compensation order under the DPA 2018 or damages for a breach of the Human Rights Act 1998.

A full list of the exemptions can be found at the website of the Information Commissioners Office http://www.ico.org.uk/for_organisations/data_protection/the_guide/exemptions

11.1 Organisational responsibilities

Each partner organisation is responsible for making sure that their organisational and security measures protect the lawful use, confidentiality, integrity and availability of information shared under this Protocol.

- Partner organisations will accept the security classifications on information and handle the information accordingly.
- Partner organisations accept responsibility for auditing compliance with the information sharing agreements in which they are involved.
- Partner organisations should make it a condition of employment that its employees will abide by its rules and policies on the protection and use of confidential information

and will have relevant training, procedures and checks (such as DBR checks) in place for all staff.

- Partner organisations should make sure that their contracts with external service providers abide by their rules and policies on the protection and use of confidential information.
- The partner organisation originally supplying the information (Data Controller) should be notified promptly of any breach of confidentiality, or incident, involving a risk or breach of the security of information (see Section 9. Personal Data Breaches).
- Partner organisations should have documented policies for records retention, maintenance and secure waste destruction.

11.2 Individual responsibilities

Every employee working for the organisations listed in this Partnership Agreement:

- is personally responsible for the safekeeping of sensitive information they obtain, handle, use and disclose.
- should know how to obtain, use and share information they legitimately need to do their job.
- has an obligation to request proof of identity, or take steps to validate the authorisation of another before disclosing sensitive information.
- must uphold the general principles of confidentiality and data protection as outlined by the GDPR (Appendix 4), DPA 2018 (Appendix 5) and the Caldicott Review 2013 (Appendix 6), follow the policies and procedures of their organisation, this Protocol and seek advice when necessary.
- should be aware that any violation of privacy or breach of confidentiality is unlawful and may be a disciplinary/criminal matter that could lead to dismissal or prosecution.
- should ensure any information is transferred using an approved, secure method of transportation in accordance with their organisation's policies and procedures.
- must ensure they follow their own organisation's policies and procedures before releasing any information under this Agreement.

12. Protocol Signatories

Members of the Derbyshire Partnership Forum (DPF) have agreed to abide by the terms of this Protocol, its appendices and any variations to the Protocol or its appendices. The latest list of DPF members is available on the Derbyshire Partnership Forum website.

Appendix 1 – Glossary

Anonymised Data - This is data which does not identify an individual directly, and which cannot reasonably be used to determine identity. Anonymisation requires the removal of name, address, full postcode and any other detail or combination of details that might support identification.

Caldicott Guardian - a senior person in the NHS or Local Authority with responsibility for Public Health and/or Social Care who is responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information sharing.

Data - Within this Protocol data could include personal and/or sensitive personal data

Data Controller - a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Data Processor - in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Data Protection Officer (DPO) – Is responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements.

Data Recipient - in relation to personal data, means any person to whom the data are disclosed

Data Source - the source the data was originally obtained from

Data Subject - means an individual who is the subject of personal data

Disclosure - the divulging or provision of access to data.

Explicit Consent - this means articulated agreement and relates to a clear and voluntary indication of preference of choice, usually given orally or in writing and freely given in circumstances where the available options and the consequences have been made clear.

Implied Consent - This means agreement that has been signalled by the behaviour of an individual with whom a discussion has been held about the issues and therefore understands the implications of the disclosure of data.

Note: All consent must now be explicit.

Information Commissioner - The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals https://ico.org.uk

Information Governance Toolkit - Is an online system which allows NHS and Social Care organisations and partners to assess themselves against Department of Health Information Governance policies and standards. It also allows members of the public to view participating organisations' IG Toolkit assessments.

Information Sharing Protocol - Is the high level document setting out the general reasons and principles for sharing data. The protocol will show that all signatory organisations are committed to maintaining agreed standards on handling data and will publish a list of senior signatories. It should be underpinned by data sharing agreements between the organisations who are actually sharing the data.

Information Sharing Agreement (ISA) - Is a document which details the organisations approach to data sharing. Agreements will be produced where organisations specifically identify a purpose to share data across organisational boundaries. The agreement should state whether partners are obliged to, or are merely enabled to, share data.

Organisations - Used in the context of this document to relate to the organisations specified within section 12 of this Protocol which details the organisations that are signatories to this Protocol.

Personal Data - means any information relating to an identified or identifiable natural person ('data subject') who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see Article 10 of the GDPR). https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/criminal-offence-data/

Pseudonymisation - "Pseudonymisation" of data means replacing any identifying characteristics of data with a pseudonym, or, in other words, a value which does not allow the data subject to be directly identified However, pseudonymisation can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Personal data breach - A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Senior Information Risk Owner (SIRO) – Is in Senior Management and is accountable for information risks and incidents for the organisation. The SIRO will foster a culture of protecting and using data and is concerned with the management of all information assets.

Sensitive Personal Data - means any information relating to an identified or identifiable natural person ('data subject') who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, reflecting changes in technology and the way organisations collect information about people. For example, information about an individual's:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sex life, or
- sexual orientation.

The GDPR refers to sensitive personal data as "special categories of personal data" (see Article 9 of the GDPR). https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

Appendix 2 - Information Sharing Agreement Template

[Insert Additional Organisational Logo(s)]

[Title of agreement]
Information Sharing Agreement

Based on the Derbyshire Partnership Forum Information Sharing Protocol v 5.1

All Information Sharing Agreements must be sent to [the organisation] Information Governance or Legal Department for initial review and registration.

Document Status

Version	[insert…Latest version number of the ISA]
Document owner	[insert…Organisation name]
Document author and enquiry point	[insert…Name] [Job Title] [Contact Details]
Document authoriser	[insert… Name and Job Title of whomever has approved this ISA i.e. Director, Head of Service, DPO, Caldicott Guardian etc.]
Document agreed date	[insert…date all parties have agreed and signed up to the ISA]
Document classification	[insert…Public / Controlled / Restricted]
Document distribution	[insert…list partners organisations]
Document retention period	[insert…for example: 3 years from document review/end date]
Next document review/end date	[insert… date appropriate for this ISA which may depend on your data, 1 or 2 years or change to data and or data processors and sub processors in which case a whole document review may be required and possibly a revised Privacy Impact Assessment]

Version History

Date Issued	Version	Status	Reason for change

See Derbyshire Partnership Forum Information Sharing Protocol version 5.0 for guidance on completion. http://www.derbyshirepartnership.gov.uk/about_us/

1. Introduction

Insert a brief introduction, examples below. Set out any Term and abbreviations here also

1.1 This Information Sharing Agreement (Agreement) has been developed to facilitate partnership working between the partners identified in 2.1 below (Parties}. This Agreement identifies the legal powers and methods of sharing information in order to achieve common goals for the benefit of the Derbyshire Area.

1.2 This Agreement outlines the need for [insert] to work together to [insert] etc.

1.3 All Parties to this Agreement should ensure that all of their staff who are affected by it are aware of its contents and the obligations it creates between the Parties signed up to it.

2. Partner and partner responsibilities

2.1 The Parties committed to this Agreement are:

Who are the intended Partners to this Agreement and what are their responsibilities? Including Data Controller, Data Processor and Sub Data Processors (third parties)

- [name of organisation] who has the role of Data Controller
- [name of organisation(s)] who has the role of Data Processor(s)
- [name of organisation(s)] who has the role of Data Sub-processor(s) - remove if not applicable

2.2 It will be the responsibility of these Parties to ensure that they:

- have realistic expectations from the outset
- maintain ethical standards
- have a process by which the flow of information can be controlled
- provide appropriate training
- have adequate arrangements to test compliance with the agreement
- meet Data Protection Act 2018 (DPA), General Data Protection Regulation (GDPR) and other relevant legislative requirements.

3. Background and scope of the Agreement

What is the purpose of the agreement? What is the specific business need/objective for information sharing? What are the benefits to sharing these data? Has a Privacy Impact Assessment (PIA) been carried out on this business process? If not, start with your organisations PIA screening questions.

3.1. It has been identified that in order to…

3.2. The Agreement covers the sharing of personal data about data subjects for the purpose of [Enter here] and the Agreement covers sharing for any of the purposes listed in Section 5: 'Purposes and legal basis for Sharing Information'.

4. Information to be shared

What specific information is required for the purpose of this agreement? List fields of Information to be shared, do these cover special categories of data, personal data? Give consideration to the identifiability of individuals. (See section 4 of the Protocol for more information on types of data). Could list in a table…

4.1 Data to be shared

4.1.1. It has been identified by the Parties that the following fields of data are required to fulfil the purpose and scope of the Agreement as identified in 3.1 and 3.2.

4.1.2. These data are to be provided by [enter Party one here] and are to be received by [enter other Party / All remaining Parties]. If any third party processing via a sub processor, detail it here also.

4.2 Data Processing

Detail any processing of the data to be carried out by any of the Parties. In particular, document processing of any special categories of personal data.

4.3 Terms of use of the information

Add a clear statement of how the information is intended to be used and any restrictions which may apply. Consider the enhanced rights of the individual, take Consent and the Right to be forgotten into consideration. Is there a Privacy Notice in place for these data? If so, does this Agreement fit with the agreed terms of re-use (if any)? Could also specify named individuals who would be the responsible for processing the data etc.

4.4 Exchange of Information

State explicitly how and what information is to be shared, consider methods such as encrypted email, mail, secure file transfers and how regularly these are to take place.

5. Purposes and legal basis for information sharing

5.1 Purpose for sharing information

5.1.1. The main purpose for sharing information is to… how will services be improved, what value does the data have, what value will be added by any data processing activity?

5.2 Legal Basis for Sharing Information

5.2.1. The legal basis for sharing information between the Parties has been identified as …State Legal basis for information sharing. What are the specific lawful powers/obligations for the processing of information?

What considerations apply to make the processing fair under the terms of the Data Protection Act 2018 or GDPR? (see Appendix 4 and 5 of the Derbyshire Partnership Information Sharing Protocol (https://www.derbyshirepartnership.gov.uk/site-

elements/documents/pdf/information-sharing-protocol.pdf) or for full DPA 2018 visit http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf.

5.3 Other legislation which has an impact on the Agreement

Could include a brief description of the main impact of relevant legalisation and can have an appendix to list all relevant legislation (if applicable), see Appendix 3 of the Derbyshire Partnership Information Sharing Protocol for examples of other legalisation that could be considered.

6. Data Quality

Explain what standards will apply for data quality and how errors will be handled. Taking the GDPR principles and rights for individuals into consideration as well as principles 3 and 4 of the DPA 2018 (see Appendix 4 and 5 of the Derbyshire Partnership Information Sharing Protocol), for example:

6.1. Information shared under this Agreement must be fit for purpose, meaning that it must be adequate, relevant and not contain excessive detail which is beyond that required for the agreed purpose.

6.2 Where information received by any partner is insufficient to achieve the agreed purpose, i.e. inaccurate, out-of-date or inadequate for the stated purpose clarification will be sought with the Data Controller before the information is acted upon. Partner's receiving such queries will act promptly to resolve them, ensuring corrections are documented and cascaded to all Parties without delay.

Appropriate records will be kept to record sources of information and any methodologies applied when processing the data.

7. Retention, Storage and Disposal

Explain how long the information is intended to be retained for the purpose, how the data will be stored and any specific security, review or disposal arrangements that apply.

7.1 State explicitly how long the data is to be held for by all Parties if the Data Controller intends for the Data Processors to only keep these data for a specified period in accordance with the Data Controllers retention policy, otherwise could say in line you're your organisations retention policies.

7.2 All Parties must ensure that they have appropriate measures in place to ensure the secure storage of all the information subject to this Agreement will be kept as follows:

- Physical copies of information provided should be held in a lockable storage area, office or cabinet
- Electronic files must be protected against illicit internal use or intrusion by external parties through the appropriate security measures

7.3 How are the Parties expected to dispose of the data at the end of the retention period?

8. Access and Security

Explain the standards and conditions which are required to protect the information concerned. Include any special arrangements which might apply. For example access to files will be restricted – operate a clear desk policy, employees given access on a need to know basis. Is there any specific training needed or is a basic or enhanced Disclosure and Barring Service (DBS) check required?

9. Handling of complaints, information requests or breaches of the Agreement

9.1 Handling of data breaches

9.1.1. Data processors, will in the event of a personal data breach or breach of confidentiality take steps to notify the Data Controller and relevant organisations Data Protection Officer(s) (DPO) as soon as possible. The Data Controller has the responsibility to notify the ICO of a serious breach within 72 hours of any signatory organisations becoming aware of the breach. See section 9 of the Protocol for more information.

Detail the relevant DPO contact information. Organisation will be required to record all information about any personal data breaches.

9.2 Indemnity to the Agreement

9.2.1. Each Party will keep each of the other Parties fully indemnified against any and all costs, expenses and claims that arise out of any breach of this Agreement by their staff, agent, contractors or data processors and in particular, but without limitation, the unauthorised or unlawful loss, theft, use, destruction or disclosure by the offending Parties or its sub-contractors, data processors, employees, agents or any other person within the control of the offending Parties of any data obtained in connection with this Agreement.

9.3 Handling of complaints

9.3.1 Any Party, on receipt of a complaint, without delay must…

9.4 Handling of requests for information under Data Protection / FOI

9.4.1 Where the [non Data Controller], in response for [insert] information made under the Freedom of Information Act 2000, or the Environmental Information Regulations 2004 or a Subject Access Request, as applicable is considering disclosing [insert] information obtained via this Agreement it will consult with [Data Controller] before doing so.

9.4.2 The [non Data Controller] will, in fulfilling obligations under the Freedom of Information Act 2000 or the Environmental Information Regulations 2004, or Subject Access Request, as applicable, comply with the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) where the [insert] information includes personal and/or special category data.

10. Commencement and Termination of the Agreement

10.1 Commencement of the Agreement

10.1.1 This Agreement shall take effect from the date that the Parties fix their signatures below and shall continue in force for as long as the pilot phase continues or until this Agreement is terminated under Section 10.2 below.

Termination of the Agreement

10.2.1 Any Party may terminate this Agreement at any time provided they give a minimum of 30 days' notice in writing to the other Parties.

10.2.2 Any Party can suspend this Agreement for 30 days if they consider that security arrangements have been compromised. Such suspension arrangements are intended to allow the affected Party the opportunity to seek a resolution and cause any remedial actions to be completed. In the event that agreement is not reached, the Agreement will be terminated in writing with full explanation to the Parties concerned.

10.2.3 The obligations of confidentiality imposed on the Parties by this Agreement shall continue in full force and effect after the expiry or termination of this Agreement.

11. Monitoring, review and dissemination of the Agreement

Detail the procedures and process for monitoring the implementation of the ISA. Specify the review period for the ISA and name the individual who will be responsible for the review process (normally the document author).

11.1 Monitoring of the Agreement

Detail the procedures and process for monitoring the application of the ISA and detail the responsibilities for monitoring of all Parties. Will the procedures, methods and data be reviewed by the Data Controller during the life of the Agreement? i.e the Audit team review the measures, training, security etc. If the process, methodology or data quality are not what the Data Controller expects…

11.2 Review of the Agreement

11.2.1 All Parties agree to review the Agreement every two years or when there is any major change to the data, process, relevant legislation or Parties to the Agreement. The Parties agree to notify a representative of the Data Controller of any requirements to review the Agreement and it will be the responsibility of the Data Controller to instigate the review.

11.3 Dissemination of the Agreement

11.3.1 All Parties will disseminate copies of this Agreement to all relevant staff and, on request, to the data subjects of the Agreement process and will ensure that appropriate training is provided to all relevant staff.

12. Signatories

Ensure all organisations have agreed to and signed the Agreement **before** information sharing takes place. Check your organisations approval procedures as it may require your Data Projection Officer (DPO), Caldicott Guardian, Senior Information Risk Officer

(SIRO), Information Governance lead officer or Director to agree and sign this Agreement.

Data Controller: Insert Organisation name

Name & Title/Role	Signature	Date

Data Processor: Insert Organisation name

Name & Title/Role	Signature	Date

Data Processor: Insert Organisation name

Name & Title/Role	Signature	Date

A word version of the template is available here
http://www.derbyshirepartnership.gov.uk/about_us/

Appendix 3 - Legal Framework

The legal framework within which public sector data sharing takes place is complex and overlapping and there is no single source of law that regulates public sector information sharing. The purpose here, therefore, is to highlight the legal framework that affects all types of personal information sharing, rather than serve as a definitive legal reference point. The general legal framework surrounding the sharing of information includes but is not limited to:

- United Kingdom Administrative Law (law that governs public bodies actions)
- Human Rights Act 1998 and the European Convention on Human Rights (Article 8.1)
- Health and Social Care (Safety and Quality) Act 2015
- General Data Protection Regulation (GPR) 2016
- Data Protection Act 2018
- Freedom of Information Act 2000;
- No secrets, Department of Health 2015
- Common Law Duty of Confidence
- Caldicott Principles 2013
- Children's Act 1989, 2004
- Children and Social Care Act 2017
- Computer Misuse Act 1990
- Crime and Disorder Act 1998
- Education Act 1996, 2002, 2005, 2011
- Health Act 1999, 2006, 2009
- Care Act 2014
- Mental Capacity Act 2005
- Mental Health Act 1983, 2007
- Mental Health (Patients in the Community) Act 1995
- NHS Data Security and Protection Toolkit
- Government Security Classifications April 2014
- Re-Use of Public Sector Information Regulations 2015
- Legislation that covers specific aspects of public service delivery (e.g. child protection, patient records)

Overall the law strikes a balance between the rights of individuals and the interests of society. The law is not a barrier to sharing information where there is an overriding public interest in doing so (such as where it is necessary to do so to protect life or prevent crime or harm) provided it is done fairly and lawfully.

Often personal information can be shared simply by informing people from the outset what purposes their information will be used for and then sharing only for those agreed purposes. There are however special legal considerations around sharing information that is personally sensitive or confidential, because this could have serious consequences for individuals. In deciding whether the law allows personal information to be shared, the following four steps should be considered (as recommended by the Ministry of Justice):

1. Establish whether there is a legal basis for sharing the information (i.e. whether the reason for sharing the information has a statutory basis – e.g. the prevention of crime) or whether there are any restrictions (statutory or otherwise) to sharing the information;

2. Decide whether the sharing of the information would interfere with human rights under the European Convention on Human Rights;

3. Decide whether sharing information would breach any common law obligations of confidence;

4. Decide whether the sharing of the information would be in accordance with the Data Protection Act 2018, in particular the Data Protection Principles, as set out in Appendix 5. In addition, the Freedom of Information Act 2000 gives anyone (an individual or an organisation) a right to request access to information from a public body. Where an exemption applies (e.g. it is third party personal information or commercially sensitive information), disclosure may be refused.

Appendix 4 – General Data Protection Regulation (GDPR)

The GDPR will apply in the UK from 25 May 2018. Under the GDPR, the data protection principles set out the main responsibilities for organisations. The principles are similar to those in the Data Protection Act 2018 (DPA), with added detail at certain points and a new **accountability** requirement which requires you to show **how** you comply with the six principles.

1. Lawfulness, fairness and transparency

Transparency: Tell the subject what data processing will be done.

Fair: What is processed must match up with how it has been described

Lawful: Processing must meet the tests described in GDPR [article 5, clause 1(a)]

2. Purpose limitations - Personal data can only be obtained for "specified, explicit and legitimate purposes"[article 5, clause 1(b)]. Data can only be used for a specific processing purpose that the subject has been made aware of and no other, without further consent. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

3. Data minimisation - Data collected on a subject should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".[article 5, clause 1(c)] i.e. No more than the minimum amount of data should be kept for specific processing.

4. Accuracy - Data must be "accurate and where necessary kept up to date" [article 5, clause 1(d)] Baselining ensures good protection and protection against identity theft. Data holders should build rectification processes into data management / archiving activities for subject data i.e. every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

5. Storage limitations - Regulator expects personal data is "kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the personal data are processed". [article 5, clause 1(e)] i.e. Data no longer required should be removed. However, personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

6. Integrity and confidentiality - Requires processors to handle data "in a manner [ensuring] appropriate security of the personal data including protection against unlawful processing or accidental loss, destruction or damage, using appropriate technical or organisational measures.". [article 5, clause 1(f)]

The GDPR creates some new rights for individuals and strengthens some of the rights that currently exist under the DPA. The GDPR provides the following eight rights for individuals:

1. Lawfulness, fairness and transparency The right to be informed encompasses your obligation to provide 'fair processing information', typically through a privacy notice. It emphasises the need for transparency over how you use personal data.

2. The right of access - Under the GDPR, individuals will have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice (see Article 15).

These are similar to existing subject access rights under the DPA.

3. The right to rectification - **When should personal data be rectified?** Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

If you have disclosed the personal data in question to third parties, you must inform them of the rectification where possible. You must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

4. The right to erasure - The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

5. The right to restrict processing - Under the DPA, individuals have a right to 'block' or suppress processing of personal data. The restriction of processing under the GDPR is similar.

When processing is restricted, you are permitted to store the personal data, but not further process it. You can retain just enough information about the individual to ensure that the restriction is respected in future.

6. The right to data portability **-** The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

7. The right to object **-** Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

8. Rights in relation to automated decision making and profiling - The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. These rights work in a similar way to existing rights under the DPA.

Identify whether any of your processing operations constitute automated decision making and consider whether you need to update your procedures to deal with the requirements of the GDPR.

Further reading on the GDPR can be found on the Information Commissioners Office website https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

Appendix 5 - Data Protection Principles

The Data Protection Act 2018 governs the protection and use of personal data. It sets out standards which must be satisfied when obtaining, recording, holding, using or disposing of personal data. These are summarised by the six Data Protection Principles. Under the key principles of the Act, personal data must be:

Principle 1 - processed fairly and lawfully. There should be no surprises – data subjects should be informed about why information about them is being collected, what it will be used for and who it may be shared with.

Principle 2 - obtained and processed for specified, explicit and legitimate purposes. Only use personal information for the purpose(s) for which it was obtained and ensure it is not processed in any other manner that would be incompatible with that purpose(s);

Principle 3 - adequate, relevant and not excessive. Only collect and keep the information you require. It is not acceptable to collect information that you do not need. Do not collect information 'just in case it might be useful one day';

Principle 4 - accurate and kept up to date. Have in place mechanisms for ensuring that information is accurate and up to date. Take care when inputting to ensure accuracy and have local procedures in place to manage requests for information to be amended;

Principle 5 - not kept for longer than is necessary. The legislation within which area you are working in, will often state how long documents should be kept. Information should be disposed of in accordance to your organisation's Records Management Policy (including retention and disposal);

Principle 6 - processed in a secure manner. Using appropriate technical or organisational measures (and, in this principle, “appropriate security” includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).

Source: Data Protection Act 2018, Part 4, Chapter 2 Data Protection Act 2018.

http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf

Appendix 6 - Caldicott Principles

The Caldicott Review 2013 re-enforced the original principles of 1997 regarding the use of client information in health and social care organisations and added a 7th principle regarding the sharing of information.

Principle 1 - Justify the purpose(s)

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian.

Principle 2 – Do not use personal confidential data unless it is absolutely necessary

Person confidential data items should not be included unless it is essential for the specified purpose (s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose (s).

Principle 3 - Use the minimum necessary personal confidential data

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

Principle 4 - Access to personal confidential data should be on a strict need to know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may been introducing access controls or splitting data flows where one data flow is used for several purposes.

Principle 5 -Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

Principle 6 - Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

Principle 7 - The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

For more information on the Seven Caldicott Principles July 2013 see https://www.igt.hscic.gov.uk/Caldicott2Principles.aspx

Or for the full Caldicott Review go to: https://www.gov.uk/government/publications/the-information-governance-review

Appendix 7 - Consent: Guidance notes

Consent is one of six lawful bases to process personal data under the GDPR.

In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller. Recital 43 of the GDPR gives the example of where the controller is a public authority.

It is important, therefore, that you consider whether consent is the appropriate lawful basis to process the data or whether another ground should be chosen instead. So, if you would still need to process the data without consent, asking for such consent is misleading and unfair.

Most lawful bases require that processing is 'necessary'. If you cannot demonstrate the processing is necessary, then you are likely to require the consent of the individual as your lawful basis for processing their personal data.

Consent can only be an appropriate lawful basis if the individual is offered control and choice with regard to accepting or declining the terms offered or declining them without detriment.

When asking for consent you need to assess whether it will meet all the requirements to obtain valid consent. The requirement to establish that valid and explicit consent has been obtained is even more important in circumstances where you are processing special category data, such as data relating to health, racial origin, religious and philosophical beliefs etc.

Article 4(11) of the GDPR defines consent as: *"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmation action, signifies agreement to the processing of personal data relating to him or her."*

The GDPR stipulates that consent of the data subject means any:

- freely given
- specific
- informed and
- unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

If the individual has no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent will not be valid. If consent is bundled up as a non-negotiable part of terms and conditions, or if the individual is unable to refuse or withdraw consent without detriment it will not be freely given.

You must pay particular attention to consent forms aimed at children. These should be clearly worded and understandable in order in order to ensure that you can satisfy that you have obtained informed consent.

The following checklist will ensure that your consent form meets the standards required:

1. You have checked that consent is most appropriate lawful basis for processing.
2. You have made the request for consent prominent and separate from terms and conditions.

3. You have asked individuals to positively opt in by clear, affirmative action
4. You have not relied on pre-ticked boxes or any other type of default consent.
5. You use clear, plain language that is easy to understand.
6. You specify why you need the data and what the data will be used for.
7. You give individual or granular options to consent separately to different purposes and type of processing.
8. You name any third party controllers who will be relying on the consent.
9. You tell individuals that they can withdraw their consent at any time.
10. You ensure that individuals can refuse to consent without detriment.
11. You do not make consent a precondition of a service.
12. If you offer online services directly to children, you only seek consent if you have age-verification measures (and parental-consent measures for younger children) in place.

You must ensure that you keep a record of when and how you obtained consent and exactly what the individual was told at the time.

You should regularly review consents to check that the relationship, the processing and the purposes have not changed. You should have processes in place to refresh consent at appropriate intervals, including any parental consents. You must tell individuals that they can withdraw their consent at any time, without detriment, and you must act on withdrawal of consent promptly. It is good practice to use privacy dashboards or other preference-management tools.

You are obliged to inform individuals of their rights under data protection legislation, in addition to other information, such as retention periods and the identity of the Data Protection Officer. Therefore, your consent form should include a link to your Privacy Policy on your website.

Capacity to consent

For a person to have capacity to consent, he/she must be able to comprehend and retain the information material to the decision and must be able to weigh this information in the decision making process. See guidance as defined in the Mental Capacity Act 2005.

Consent and Children

Until recently section 8 of the Family Law Reform Act entitled young people aged 16 or 17, having capacity, to give informed consent. The courts have held that young people (below the age of 16) who have sufficient understanding and intelligence to enable them to understand fully what is involved will also have capacity to consent. This was augmented by the Fraser (previously Gillick) Competency test. However, if you are relying on consent as your lawful basis for processing personal data, when offering an online service directly to a child, only children aged 13 or over are able provide their own consent. see here for further information https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/applications/children/

It should be seen as good practice to involve the parent(s) or guardian/representative of the young person in the consent process, unless this is against the wishes of the young person. In the case where the wishes of a young person, who is deemed competent to give consent, are opposed to those of their parent/carer, then the young person's wishes should take precedence.

Recording consent - all agencies should have in place a means by which an individual, or their guardian/representative, can record their explicit consent to personal information being disclosed and any limitations, if any, they wish to place on that disclosure.

The consent form should indicate the following:

- details of the agency and person obtaining consent;
- details to identify the person whose personal details may/will be shared;
- the purpose of sharing personal information;
- the organisation(s) with whom the personal information may/will be shared;
- the type of personal information that will be shared;
- details of any sensitive information that will be shared;
- any time limit on the use of the consent;
- any limits on disclosure of personal information, as specified by the individual;
- details of the person (guardian/representative) giving consent if appropriate.

The individual or their guardian/representative, having signed the consent, should be given a copy for their retention. The consent form should be securely retained on the individual's record and relevant information should be recorded on any electronic systems used, in order to ensure that other members of staff are made aware of the consent and any limitations.

Disclosure without consent

Disclosure of personal information without consent must be justifiable on statutory grounds, or a meet the criterion for claiming an exemption under the Data Protection 2018. Without such justification, both the agency and the member of staff expose themselves to the risk of prosecution and liability.

There are exceptional circumstances in which a patient's right may be overridden, for example:

- if an individual is believed to be at serious risk of harm, or
- if there is evidence of serious public harm or risk of harm to others, or
- if there is evidence of a serious health risk to an individual, or
- if the non-disclosure would significantly prejudice the prevention, detection or prosecution of a crime, or
- if instructed to do so by a court.

In deciding whether or not disclosure of information given in confidence is justified it is necessary to weigh the harm that would result from breach of confidence against the harm that might result if you fail to disclose the information.

All agencies should designate a person(s) who has the knowledge and authority to take responsibility for making decisions on disclosure without consent. This person(s) should hold sufficient seniority within the organisation with influence on policies and procedures. Within the health and social care agencies it expected that this person will be the Caldicott Guardian.

If information is disclosed without consent, then full details will be recorded about the information disclosed, the reasons why the decision to disclose was taken, the person who authorised the disclosure and the person(s) to whom it was disclosed.

A record of the disclosure will be made in the patient's record and the patient must be informed if they have the capacity to understand, or if they do not have the capacity then any person acting on their behalf must be informed.

If information is disclosed without consent, there may be some exceptional circumstances (particularly in the context of police investigations or child protection work) where it may not be appropriate to inform the patient of the disclosure of information.

This situation could arise where the safety of a child (or possibly sometimes of an adult) would be jeopardized by informing the patient of such disclosure. In many such situations it will not be a case of never informing the patient, but rather delaying informing them until further enquiries have been made. Any decision not to inform, or to delay informing, should be recorded on the patient's record, clearly stating the reasons for the decision, and the person making that decision.

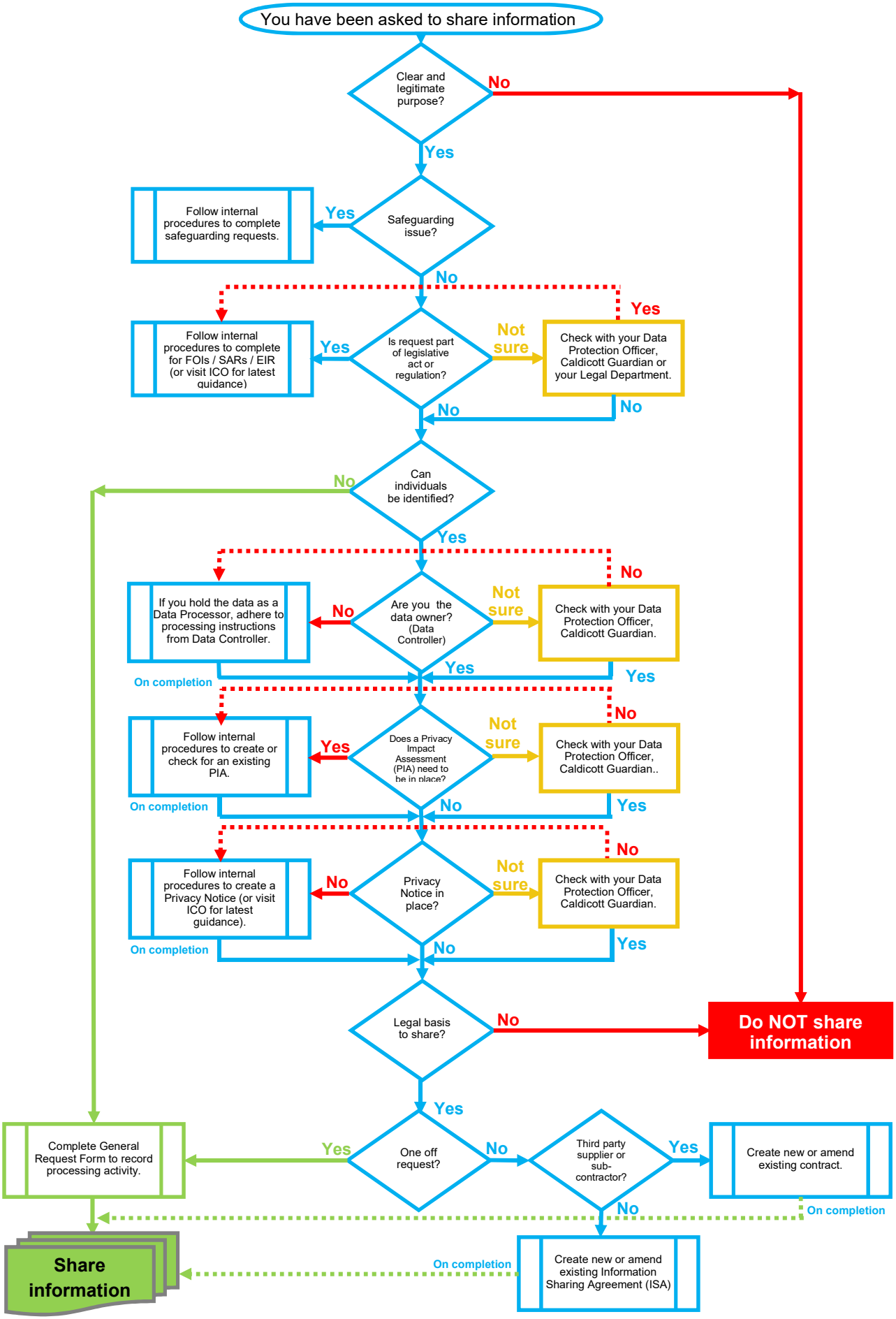
Further Reading on consent to share information

Information: To share or not to share? The Information Governance Review https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf

Information Commissioners Office (ICO): https://ico.org.uk/for-the-public/personal-information/sharing-my-info/

ICO GDPR Consent: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/consent/

Appendix 8 - Flowchart of key questions for information sharing



Explanation of some of the flowchart sections:

Is there a clear and legitimate purpose for sharing information? Whether you work for a statutory or non-statutory service, any sharing of information must comply with the law relating to confidentiality, data protection and human rights. Establishing a legitimate purpose for sharing information is essential to meet these requirements. See sections 3 to 5 of the DPF Information Sharing Protocol for more information and advice.

Is the information request about a safeguarding issue? When sharing personal information relating to an imminent safeguarding concern the safety of the individual should be your first priority. As long as you can justify your decision to share information under these circumstances and have recorded it appropriately you will not be in breach of data protection legislation. See you organisations policies and procedures on Safeguarding information.

Is the request part of a legislative act or regulation? The public have the right to request information from a Public Authority, and as such may receive requests such as Freedom of Information (FOI), Subject Access Requests (SAR) and Environmental Information Regulations (EIR) requests, there is a duty to fulfil these requests within given parameters and time limits. Check your organisations policies and procedures.

Can individuals be identified? Does the information enable a living person to be identified? If the information is anonymised, it can be shared. However, if the information is about an identifiable individual or could enable a living person to be identified when considered with other information, it is personal information and is subject to data protection and other laws. Please see the GDPR principles (Appendix 4 of the DPF Information Sharing Protocol and also see the Caldicott Review 2013 for further information and also for clarity on deceased individuals).

Do we own the data? Is this organisation the Data Controller? There are specific roles regarding data and its ownership and if we are the owner then we have the duty to control and specify how our data is handled, processed, stored and shared. If we are not the owners, then we are 'Data Processors' and as such we must adhere to the rules, guidelines and security measures stipulated by the Data Controllers and we MUST maintain records of all processing activity.

Does the request requires a Privacy Impact Assessment (PIA) to be in place? Has a PIA already been conducted on the data/project? If not, start with the PIA screening questions which will help you assess if a full PIA is required. If the answer is Yes to any of the screening questions then a PIA is required (see your organisations policies and procedures for further information on how to find existing and create new PIAs).

Is there a Privacy Notice in place? As a Data Controller we own and process hundreds of items of data and everyone now has the right to be informed about any personal information held. How we use it, who we share it with, how we keep it secure, how long we keep it for and their rights, including those about accessing their records. We have a duty to publicise this in a Privacy Notice, see your organisations policies and procedures for further information on how to find existing and create new privacy notices.

Do you have a legal basis to share information? There are six lawful basis to processing personal and/or special category data, namely: Contract, legal obligation, vital interests, public task, consent and legitimate interests, and if your organisation is a public authority then at least one of the six lawful bases must be applied whenever data are processed.

Is the request a one off or more frequent? To fulfil our purpose of sharing information between departments, professions and organisations to improve the lives of our residents we receive many requests some which are ad-hoc/one-off or some types need to become more formalised. Your organisation has policies and procedures for dealing with the differing types of information sharing and procedures to formalise the process of sharing information such as completing an Information Sharing Request Form, Information Sharing Agreement or make amendments to an existing contract with a third party:

- General requests for information – requests for information are received and sent from across the organisation and a record of what information requests we receive and how we then process the requests should be recorded, whether or not you decide to share information and the exchange formalised by all Parties via the use of the Data Sharing Request
- Data protection clauses in Third party/supplier contracts - formalisation of agreed processing activity by all Parties
- Information Sharing Agreement (ISA) – formal document detailing how data is to be processed by all Parties who are signatories to the Agreement

Share information - You have made the informed decision to share information, you should share it in a proper and timely way, act in accordance with the principles of the GDPR and DPA 2018, and follow your organisations policies and procedures for information governance and security. Take steps such as appropriate staff training, increase information security, and ensure data accuracy.

Do NOT Share information - You have made the informed decision to NOT share information, for reasons such as no legal basis or the data requested is not relevant to the purpose requested for example. Your decision and the reasons why you have not shared the data should be recorded for future reference so others can check the decision made (occasionally the same request can be received via multiple avenues), it is good practice to use a Data Sharing Request Form to record your decision.

Source: This flowchart has been adapted from the Derbyshire County Council Information Sharing Policy and Guidance document v1.0.